Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

Helmut Hasse

Band 176

Heft 1

Ausgegeben am 21. Oktober 1936

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung / J. Guttentag, Verlagsbuchhandlung / Georg Reimer / Karl J. Trübner / Veit & Comp.

Berlin W 35 und Leipzig

1936

Band 176. Heft 1.

Inhaltsverzeichnis.

	Seite
Wegner, Udo, Bestimmung eines auflösbaren Körpers vom Primzahlgrad aus der Form seiner Diskriminante	1
Hasse, Helmut, Über die Diskriminante auflösbarer Körper von Primzahlgrad	12
Denk, Franz, Über den Aufbau der Permutationen geordneter Elemente	18
Broggi, Ugo, Su due sistemi associati di infinite equazioni lineari	25
Witt, Ernst, Theorie der quadratischen Formen in beliebigen Körpern	31
Vassiliou, Ph., Über affektlose Gleichungen	45
Aumann, Georg, Vollkommene Funktionalmittel und gewisse Kegelschnitteigenschaften	49
Lubelski, S., Zur Gaußschen Kompositionstheorie der binären quadratischen Formen	56

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgendeinem Grunde Textänderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von Abhandlungen bis zu 24 Seiten Umfang 75 Sonderabdrucke, von größeren Arbeiten 50 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Redaktion unter der Adresse:
An die Redaktion des Journals für die reine und angewandte Mathematik
Professor Dr. Helmut Hasse, Göttingen, Mathematisches Institut, Bunsenstr. 3-5.

Druck von Walter de Gruyter & Co., Berlin W 35
Printed in Germany

Bestimmung eines auflösbaren Körpers von Primzahlgrad aus der Form seiner Diskriminante.

Von *Udo Wegner* in Darmstadt.

In einer früheren Arbeit [1]) habe ich unter anderem gezeigt, daß die Diskriminante $\vartheta_{K/P}$ eines binomischen Körpers $K = P(\sqrt[p]{a})$ vom Primzahlgrad p über dem Körper P der rationalen Zahlen, als Hauptideal in P geschrieben (also bis aufs Vorzeichen), die Form hat:

$$\vartheta_{K/P} = p^{p-2}\, p^m\, (p_1 \cdots p_n)^{p-1} = p^{p-2}\, p^m\, a_0^{p-1}, \qquad p_\mu \neq p_\nu, p,$$

wobei m einen der folgenden drei Werte hat:

$$\alpha) \quad m = 0,$$
$$\beta) \quad m = 2,$$
$$\gamma) \quad m = p + 1.$$

Hierbei ist im Falle α) und β)

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \qquad \text{mit} \quad \alpha_\nu \not\equiv 0 \bmod p$$

[und zwar tritt Fall α) auf, wenn $a^p \equiv a \bmod p^2$ ist, und Fall β), wenn $a^p \not\equiv a \bmod p^2$ ist], und im Falle γ)

$$a = p^{\varkappa} p_1^{\alpha_1} \cdots p_n^{\alpha_n} \qquad \text{mit} \quad \alpha, \alpha_\nu \not\equiv 0 \bmod p.$$

Es erhebt sich nun die interessante Frage, ob umgekehrt jeder auflösbare algebraische Zahlkörper vom Primzahlgrad p ein binomischer Körper ist, wenn seine Diskriminante die Form $p^{p-2}\, p^m\, (p_1 \cdots p_n)^{p-1}$ hat, wo m eine der Zahlen $0, 2, p+1$ bedeutet. Unter gewissen ziemlich einschränkenden Voraussetzungen bezüglich der p_ν konnte ich diese Frage in bejahendem Sinne beantworten [2]). Im folgenden will ich zeigen, daß diese Voraussetzungen wesentlich reduziert werden können. Es gilt nämlich der folgende

Satz. *Ist* K *ein auflösbarer Körper vom Primzahlgrad* p *über* P, *und ist die Diskriminante*

$$\vartheta_{K/P} = p^{p-2} \begin{Bmatrix} p^0 & a_0^{p-1} \\ p^2 & a_0^{p-1} \\ p^{p+1} & a_0^{p-1} \end{Bmatrix},$$

[1]) U. Wegner, Zur Theorie der auflösbaren Gleichungen von Primzahlgrad. I, Journal f. reine u. angew. Math. **168** (1932), S. 176—192.

[2]) Siehe [1]), S. 189. — Im Beweis des Satzes auf S. 190, Zeile 5, muß λ eine p-te Idealpotenzzahl und keine Einheit darstellen, worauf Herr A. Scholz freundlicherweise aufmerksam machte. Der Beweis bleibt dabei fast wörtlich bestehen. Ich führe ihn kurz an. Aus $\mu = p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n} \lambda$ und $S(\mu) = \mu^{\varkappa} \alpha^p$ (in den dortigen Bezeichnungen) folgt dann durch Normbildung $\varkappa = 1$ und dann durch wiederholtes Anwenden von S auf $S(\lambda) = \lambda \alpha_1^p$ weiter $N(\lambda) = \lambda^{p-1} \beta^p$, d. h. $\lambda^{-1} = N(\lambda) \gamma^p$. Also darf μ rational angenommen werden.

wo a_0 ein Produkt von verschiedenen Primzahlen $p_\nu \neq p, 2$ ist, deren Anzahl im ersten Falle mindestens 1 ist und für die in diesem ersten Falle die $e_\nu = \frac{p-1}{f_\nu}$ (f_ν der Exponent von p_ν mod. p) *teilerfremd sind, so ist* $\mathsf{K} = \mathsf{P}(\sqrt[p]{a})$ *mit rationalem a, also* K *ein binomischer Körper* [3]).

Beweis. Sei K ein über dem rationalen Zahlkörper P auflösbarer Körper vom Primzahlgrad p und N der kleinste K enthaltende Normalkörper über P. Dann wird N gebildet als Produkt von K und einem zyklischen Körper Z vom Grade $\frac{p-1}{\varkappa}$, wo $\varkappa$ ein Teiler von $p-1$ ist. Denn die Galoissche Gruppe $\mathfrak{G}$ ist ein Teiler der vollen linearen Gruppe des Grades p und der Ordnung $p(p-1)$. $\mathfrak{G}$ wird erzeugt durch zwei Substitutionen S und $T^\varkappa$, wobei

$$S^p = T^{p-1} = E \quad \text{und} \quad ST = TS^r$$

ist (r eine Primitivwurzel mod. p). $\mathfrak{G}$ besitzt eine invariante Untergruppe der Ordnung p, nämlich den durch S erzeugten Zyklus [4]).

A. Wir behaupten, daß $\varkappa = 1$ ist.

Im Falle α) schließt man wie folgt: In K ist [5])

$$(p) = \bar{\mathfrak{q}}_1(\mathfrak{q}_1 \cdots \mathfrak{q}_e)^b \left\{ \begin{array}{l} \bar{\mathfrak{q}}_1 \text{ vom Grade } 1 \\ \mathfrak{q}_\nu \text{ vom Grade } f = \frac{p-1}{eb} \end{array} \right\}.$$

Wegen $(b, p) = 1$ ist $\vartheta_{\mathsf{K}/\mathsf{P}}$ genau durch $p^{ef(b-1)}$ teilbar. Nach Voraussetzung ist demnach

$$ef(b-1) = p-2.$$

Da andrerseits

$$efb = p-1$$

ist, muß $ef = 1$, also $e = 1$, $f = 1$, $b = p-1$ sein. In Z ist nun [6])

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_a)^b, \quad \mathfrak{p}_\nu \text{ vom Grade } f = \frac{p-1}{\varkappa ab}, \quad \varkappa a = e.$$

Zusammengenommen ergibt sich also $\varkappa = 1$.

Für später vermerken wir noch, daß aus den erhaltenen Zerlegungen

$$(p) = \bar{\mathfrak{q}}_1 \mathfrak{q}_1^{p-1} \text{ in } \mathsf{K}, \quad (p) = \mathfrak{p}^{p-1} \text{ in } \mathsf{Z}$$

die Unverzweigtheit von $\mathfrak{p}$ in N folgt, so daß also $\mathfrak{p}$ im Falle α) nicht in $\vartheta_{\mathsf{Z}/\mathsf{P}}$ vorkommt.

Im Falle β) und γ) ergibt sich unsere Behauptung durch Vergleich der allgemeinen Diskriminantenformel

$$\vartheta_{\mathsf{N}/\mathsf{P}} = \vartheta_{\mathsf{Z}/\mathsf{P}}^n \cdot N_{\mathsf{Z}/\mathsf{P}}(\vartheta_{\mathsf{N}/\mathsf{P}})$$

---

[3]) Schon an dieser Stelle möchte ich Herrn Hasse meinen besten Dank sagen für das große Interesse, das er dieser Arbeit entgegenbrachte, und für die vielen Ratschläge, die er mir erteilte. Insbesondere danke ich ihm für den Beweis, daß man die zum ersten Fall gemachten Voraussetzungen im zweiten und dritten Fall entbehren kann.

[4]) Siehe [1]), S. 177.

[5]) Siehe F. K. Schmidt, Zur Theorie der algebraisch auflösbaren Polynome und Zahlkörper von Primzahlgrad, Sitzungsber. d. Heidelberger Akad. 1929, Math.-nat. Kl., 2. Abhdl., S. 3—10; ferner [1]), S. 179; außerdem I. Porusch, Die Arithmetik in Zahlkörpern, deren zugehörige Galoissche Körper spezielle metabelsche Gruppen besitzen, auf klassenkörpertheoretischer Grundlage, Math. Zeitschr. **37** (1933), S. 134—160. — Letztere Arbeit zitiere ich nachstehend mit P.

[6]) Siehe [1]), S. 179, und P, S. 140.

mit der in unserem Falle gültigen speziellen Diskriminantenformel [7])

$$\vartheta_{N/P} = \vartheta_{K/P}^{\frac{p-1}{\varkappa}} \cdot \vartheta_{Z/P}.$$

Da $\vartheta_{K/P}$ nach Voraussetzung genau durch p^{p+s} teilbar ist, mit $s = 0$ im Falle β), $s = p-1$ im Falle γ), so ist jetzt p nach dem Dedekindschen Diskriminantensatz notwendig eine für K irreguläre Primzahl im Sinne dieses Satzes, und daher notwendig

$$(p) = \mathfrak{q}^p, \quad \mathfrak{q} \text{ vom Grade } 1$$

in K. Ist wieder

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_a)^b, \quad \mathfrak{p}_\nu \text{ vom Grade } f = \frac{p-1}{\varkappa ab}$$

in Z, so ist also notwendig jedes der Primideale $\mathfrak{p}_\nu$ in N verzweigt und somit in $\vartheta_{N/Z}$ enthalten. Nach einem bekannten Satz über relativ-zyklische Körper von Primzahlgrad ist $\vartheta_{N/Z}$ dann genau durch $(\mathfrak{p}_1 \cdots \mathfrak{p}_a)^{(p-1)(v+1)}$ teilbar (mit $1 \leqq v \leqq \frac{bp}{p-1}$ und $(v, p) = 1$ oder $v = \frac{bp}{p-1}$). Demnach ist $N_{Z/P}(\vartheta_{N/Z})$ genau durch $p^{af(p-1)(v+1)}$ teilbar. Da $\vartheta_{Z/P}$ wegen $(b, p) = 1$ genau durch $p^{af(b-1)}$ teilbar ist, wird $\vartheta_{N/P}$ nach der ersten Diskriminantenformel genau durch p^E teilbar, wo

$$E = af(p-1)(v+1) + af(b-1)p$$

ist. Andrerseits ist nach der zweiten Diskriminantenformel

$$E = (p+s)\frac{p-1}{\varkappa} + af(b-1)$$

$$= afb(p+s) + af(b-1), \quad \text{wegen } f = \frac{p-1}{\varkappa ab}.$$

Der Vergleich ergibt nach Division mit af:

$$(p-1)(v+1) + (b-1)p = b(p+s) + (b-1)$$

oder also

$$(p-1)(v+b) = b(p+s).$$

$$v + b = \frac{b}{p-1}(p+s).$$

Wegen $s = 0$ oder $p-1$ ist hiernach $p-1 | b$, was mit $b | p-1$ zusammen $b = p-1$ ergibt. Dies hat $\varkappa = 1$ zur Folge.

Für später vermerken wir noch die sich weiter ergebenden Tatsachen $a = 1$, also $(p) = \mathfrak{p}^{p-1}$ in Z, sowie $v + 1 = s + 2 = 2$ oder $p+1$, so daß also $\vartheta_{N/Z}$ genau durch $\mathfrak{p}^{2(p-1)}$ oder $\mathfrak{p}^{(p+1)(p-1)}$ teilbar ist, je nachdem Fall β) oder Fall γ) vorliegt.

B. In der Diskriminante von Z geht nur die Primzahl p auf. (Läßt man die gemachte Voraussetzung fallen, daß die $p_\nu \neq 2$ sein sollen, so geht unter Umständen auch noch die Primzahl 2 in der Diskriminante von Z auf.)

Da $\vartheta_{Z/P}$ Teiler von $\vartheta_{N/P}$ ist und $\vartheta_{N/P}$ bekanntlich aus genau denselben Primzahlen zusammengesetzt ist wie $\vartheta_{K/P}$, so gehen in $\vartheta_{Z/P}$ außer p höchstens die in der Voraussetzung genannten Primteiler p_ν von a_0 auf.

Wir zeigen zunächst, daß für diese p_ν die Zerlegung in K

$$(p_\nu) = \mathfrak{q}^p$$

---

[7]) Siehe [1]), S. 183, Zeile 2, und P, S. 150, sowie die nachstehende Arbeit von H. Hasse.

lautet. Falls p_ν eine für K reguläre Primzahl ist, ergibt sich dies wieder ohne weiteres aus dem Dedekindschen Diskriminantensatz und der Voraussetzung, daß $\vartheta_{K/P}$ genau durch $p_\nu^{\nu-1}$ teilbar ist.

Allgemein sei

$$(p_\nu) = (\mathfrak{p}_1 \cdots \mathfrak{p}_a)^b, \qquad \mathfrak{p}_i \text{ vom Grade } f = \frac{p-1}{ab}$$

in Z. Dann geht p_ν in $\vartheta_{Z/P}$ genau zum Exponenten $af(b-1+\varrho)$ auf, wo $\varrho \geqq 0$ die zugehörige Supplementzahl ist. Angenommen nun, die Primteiler $\mathfrak{p}_i$ gingen nicht in der Relativdiskriminante $\vartheta_{N/Z}$ auf. Dann wird

$$(p_\nu) = (\mathfrak{P}_1 \cdots \mathfrak{P}_c)^b$$

in N, und wegen

$$\vartheta_{N/P} = \vartheta_{Z/P}^n \cdot N_{Z/P}(\vartheta_{N/Z})$$

geht p_ν in $\vartheta_{N/P}$ genau zum Exponenten

$$E = paf(b-1+\varrho)$$

auf. Durch Vergleich mit

$$\vartheta_{N/P} = \vartheta_{K/P}^{n-1} \cdot \vartheta_{Z/P},$$

also

$$E = (p-1)(p-1) + af(b-1+\varrho),$$

folgt

$$af(b-1+\varrho) = p-1,$$

was wegen

$$afb = p-1$$

für die Supplementzahl ϱ den Wert

$$\varrho = 1$$

ergibt. Andrerseits ist nun nach der Diskriminantenformel der Hilbertschen Theorie des galoisschen Zahlkörpers für den zyklischen Körper Z die zu p_ν gehörige Supplementzahl ϱ gegeben durch

$$\varrho = (1-p_\nu^l) + L(p_\nu^l - p_\nu^{l-1}) + \bar{L}(p_\nu^{l-1} - p_\nu^{l-2}) + \cdots + \overset{(l-1)}{L}(p_\nu - 1),$$

wo p_ν^l die Ordnung der (ersten) Verzweigungsgruppe (also der Beitrag der Primzahl p_ν zu b) ist und $L, \bar{L}, \ldots, \overset{(l-1)}{L}$ die zu den einzelnen Verzweigungsgruppen der Ordnungen $p_\nu^l, p_\nu^{l-1}, \ldots, p_\nu$ gehörigen Exponenten sind, die jedenfalls die Ungleichungen

$$1 < L < \bar{L} < \cdots < \overset{(l-1)}{L}$$

erfüllen. Daraus und aus $\varrho = 1$ ergibt sich hier die Ungleichung

$$1 \geqq (1-p_\nu^l) + L(p_\nu^l - 1) = (L-1)(p_\nu^l - 1),$$

die nur für $L = 1$, $p_\nu = 2$, $l = 1$ möglich ist. Da wir $p_\nu \neq 2$ vorausgesetzt hatten, ist also die Annahme $\mathfrak{p}_i \nmid \vartheta_{N/Z}$ unzutreffend, und somit ist $\mathfrak{p}_i | \vartheta_{N/Z}$. Daher zerfallen die $\mathfrak{p}_\nu$ in N nach dem Gesetz $\mathfrak{p}_i = \mathfrak{P}_i^p$, und daraus folgt ohne weiteres, daß p_ν in K nach dem Gesetz $(p_\nu) = \mathfrak{q}^p$ zerfällt.

Aus dieser nunmehr für jedes p_ν bewiesenen Tatsache ergibt sich bekanntlich weiter [8]), daß p_ν in N die Zerlegung

$$(p_\nu) = (\mathfrak{P}_1 \cdots \mathfrak{P}_a)^p$$

hat, während durch Eintragen von $\mathfrak{p}_i = \mathfrak{P}_i^p$ in obige Zerlegung von p_ν in Z die Zerlegung

$$(p_\nu) = (\mathfrak{P}_1 \cdots \mathfrak{P}_a)^{bp}$$

in N folgt. Demnach ergibt sich $b = 1$, und daher geht p_ν nicht in $\vartheta_{\mathsf{Z/P}}$ auf, wie behauptet.

Für später vermerken wir noch, daß die $\mathfrak{p}_i$ als für $\mathsf{N/Z}$ reguläre Primideale in $\vartheta_{\mathsf{N/Z}}$ genau zum Exponenten $p - 1$ aufgehen, so daß also mit Rücksicht auf $b = 1$ jedes p_ν zu $\vartheta_{\mathsf{N/Z}}$ den Beitrag p_ν^{p-1} liefert.

Läßt man auch $p_\nu = 2$ zu und berechnet den Beitrag, den die Primzahl 2 in dem eben behandelten Falle $\mathfrak{p}_i \nmid \vartheta_{\mathsf{N/Z}}$ zum Führer von Z liefert [9]), so ergibt sich 2^2. Allgemein gilt also:

$\mathsf{Z/P}$ *ist ein zyklischer Körper vom Grade* $p - 1$, *dessen Führer entweder* p *oder* $4p$ *ist.*

Nach der Theorie der alsolut-abelschen Körper besagt das:

Z *ist entweder der Körper der* p*-ten Einheitswurzeln oder ein im Körper der* $4p$*-ten (aber nicht schon der* p*-ten) Einheitswurzeln enthaltener zyklischer Körper vom Grade* $p - 1$.

Je nachdem $p \equiv 1$ oder -1 mod. 4 ist, gibt es nur einen solchen Körper vom Führer $4p$ oder zwei.

Unter unserer Voraussetzung, daß die Primzahl 2 *nicht in* a_0 *vorkommt, ist stets* $\mathsf{Z} = \mathsf{P}(\zeta)$ *der Körper der* p*-ten Einheitswurzeln.*

Ich möchte diese letztere Tatsache noch ganz elementar, ohne Benutzung der Theorie der absolut-abelschen Körper, aus der erhaltenen Feststellung folgern, daß $\vartheta_{\mathsf{Z/P}}$ nur die Primzahl p enthält.

Z ist als Produkt zyklischer Körper Z_λ von Primzahlpotenzgraden $t_\lambda^{u_\lambda}$ darstellbar, mit $t_\lambda^{u_\lambda} | p - 1$. Zu einem dieser Körper Z_λ adjungieren wir den Teilkörper K_λ gleichen Grades des Körpers $\mathsf{P}(\zeta)$ der p-ten Einheitswurzeln. Der so entstehende zusammengesetzte Körper M_λ ist von einem Grade $t_\lambda^{u_\lambda + v_\lambda}$. Ein in p aufgehendes Primideal $\mathfrak{p}$ von M_λ geht mindestens zum Exponenten $t_\lambda^{u_\lambda}$ in p auf, da (p) in $\mathsf{P}(\zeta)$ die $(p-1)$-te Potenz eines Primideals, in K_λ also die $t_\lambda^{u_\lambda}$-te Potenz eines Primideals ist. Wegen $(t_\lambda, u_\lambda) = 1$ ist M_λ selbst der Verzweigungskörper für $\mathfrak{p}$ in M_λ, und als solcher relativ-zyklisch über dem Trägheitskörper für $\mathfrak{p}$. Die Diskriminante dieses Trägheitskörpers enthält die Primzahl p nicht, und da auch keine anderen Primzahlen in der Diskriminante vorkommen, ist er gleich P. Somit ist M_λ zyklisch über P. Nun existieren aber in M_λ keine zyklischen Teilkörper von höherem Grade als $t_\lambda^{u_\lambda}$. Daher ist M_λ selbst vom Grade $t_\lambda^{u_\lambda}$ (obiges $v_\lambda = 0$), d. h. $\mathsf{Z}_\lambda = \mathsf{K}_\lambda$. Da hiernach alle $\mathsf{Z}_\lambda \leqq \mathsf{P}(\zeta)$ sind, folgt $\mathsf{Z} \leqq \mathsf{P}(\zeta)$, und dann wegen der Körpergrade $\mathsf{Z} = \mathsf{P}(\zeta)$, w. z. b. w.

C. Da N relativ-zyklisch vom Primzahlgrad p über $\mathsf{Z} = \mathsf{P}(\zeta)$ ist, so ist $\mathsf{N/Z}$ ein Kummerscher Körper:

$$\mathsf{N} = \mathsf{Z}(\sqrt[p]{\mu}) = \mathsf{P}(\zeta, \sqrt[p]{\mu}), \quad \mu \text{ in } \mathsf{Z}.$$

---

[8]) Siehe P, S. 140, und U. Wegner, Zur Theorie der affektlosen Gleichungen, Math. Ann. **111** (1935), S. 738, Hilfssatz.

[9]) Siehe dazu P, S. 140 und S. 149, Satz VII.

Dabei gilt als Ausdruck dafür, daß N/P galoissch ist,

$$\mu^T \underset{p}{=} \mu^k \quad \text{mit } (k, p) = 1 \text{ [10]}.$$

Wir betrachten den Führer $\mathfrak{f}_{N/Z}$ von N/Z; wir brauchen hier nur die durch den Zusammenhang mit der Relativdiskriminante von N/Z,

$$\vartheta_{N/Z} = \mathfrak{f}_{N/Z}^{p-1},$$

gegebene Bedeutung dieses Führers, nicht auch seine klassenkörpertheoretische Bedeutung. Aus der oben bereits gegebenen Bestimmung der Beiträge zu $\vartheta_{K/P}$ ergibt sich, daß entsprechend den drei Fällen α), β), γ), also entsprechend den drei Typen von $\vartheta_{K/P}$:

$$\vartheta_{K/P} = p^{p-2} \begin{Bmatrix} p^0 & a_0^{p-1} \\ p^2 & a_0^{p-1} \\ p^{p+1} & a_0^{p-1} \end{Bmatrix},$$

für $\mathfrak{f}_{N/Z}$ die folgenden drei Typen vorliegen [11]):

$$\mathfrak{f}_{N/Z} = \begin{Bmatrix} \mathfrak{p}^0 & (a_0) \\ \mathfrak{p}^2 & (a_0) \\ \mathfrak{p}^{p+1} & (a_0) \end{Bmatrix}, \qquad \text{wo } (p) = \mathfrak{p}^{p-1} \text{ in } Z.$$

Diese drei Typen haben wir jetzt näher zu diskutieren.

α) $\mathfrak{f}_{N/Z} = (a_0)$.

p_ν sei eine in a_0 vorkommende Primzahl und zuerst $p_\nu^{f_\nu} \equiv 1 \bmod. p$ mit $f_\nu e_\nu = p - 1$. Dann erzeugt T^{e_ν} die Zerlegungsgruppe eines Primteilers $\mathfrak{q}$ von p_ν in Z, es ist also $\mathfrak{q}^{T^{e_\nu}} = \mathfrak{q}$. Ist dementsprechend $\mathfrak{q}^{g(T)}$ mit $g(T)$ vom Grade $\leqq e_\nu - 1$ der Beitrag von p_ν zu μ, so folgt aus $\mu^T \underset{p}{=} \mu^k$:

$$T\, g(T) \equiv k\, g(T) \bmod. (p,\ T^{e_\nu} - 1)$$

und daraus durch e_ν-malige Iteration

$$g(T) \equiv k^{e_\nu} g(T) \bmod. p.$$

Weil $g(T) \not\equiv 0 \bmod. p$ ist, wenn p_ν in a_0 vorkommt, ergibt sich also weiter

$$k^{e_\nu} \equiv 1 \bmod. p.$$

Daraus folgt:

Ist $a_0 = p_1 \cdots p_n$ mit $n \geqq 1$ und sind die zu den p_ν gehörigen e_ν untereinander teilerfremd, so ist $k \equiv 1 \bmod. p$, also

$$\mu^T \underset{p}{=} \mu.$$

β) $\mathfrak{f}_{N/Z} = \mathfrak{p}^2(a_0)$.

Hier kann ohne eine Zusatzvoraussetzung auf $k \equiv 1 \bmod. p$, also $\mu^T \underset{p}{=} \mu$ ge-

---

[10]) Wegen der Definition von T siehe S. 2. — Unter μ^T ist die Anwendung von T auf μ verstanden. — T stellt sich als Substitution von Z in der Form $\zeta^T = \zeta^g$ dar, wo g eine Primitivwurzel mod. p ist, die nicht notwendig mit der Primitivwurzel r in der Relation $ST = TS^r$ zusammenfällt (siehe dazu die Ausführungen im letzten Teil dieser Arbeit). — Mit $\underset{p}{=}$ wird die Gleichheit bis auf p-te Zahlpotenzen in Z bezeichnet; entsprechend ist nachher $\underset{p}{\equiv}$ verstanden.

[11]) Ohne die obigen Überlegungen heranzuziehen, kann das auch aus $\vartheta_{Z/P} = p^{p-2}$ und der Diskriminantenformel entnommen werden, die sich ohne weiteres durch Elimination von $\vartheta_{N/P}$ aus den beiden oben auf S. 3 angeführten Diskriminantenformeln ergibt; man beachte dabei die Invarianz des Ideals $\vartheta_{N/Z}$ bei den Substitutionen der Galoisgruppe von Z/P. Siehe dazu auch [1]), S. 183, sowie P, S. 149, Satz VII.

schlossen werden. Es gilt hier nämlich [12])

$$\mu \underset{\mathfrak{p}}{\equiv} 1 \bmod. p, \qquad \mu \underset{\mathfrak{p}}{\not\equiv} 1 \bmod. p\mathfrak{p},$$

also

$$\mu \underset{\mathfrak{p}}{\equiv} 1 + cp \bmod. p\mathfrak{p} \quad \text{mit rationalem } c \not\equiv 0 \bmod. p.$$

Dann ist auch

$$\mu^T \underset{\mathfrak{p}}{\equiv} 1 + cp \bmod. p\mathfrak{p},$$

während

$$\mu^k \underset{\mathfrak{p}}{\equiv} (1 + cp)^k \equiv 1 + kcp \bmod. p\mathfrak{p}$$

ist. Aus $\mu^T \underset{\mathfrak{p}}{=} \mu^k$ folgt also hier

$$kc \equiv c \bmod. p,$$

wegen $c \not\equiv 0 \bmod. p$ also

$$k \equiv 1 \bmod. p.$$

$\gamma)$ $\mathfrak{f}_{N/Z} = \mathfrak{p}^{p+1}(a_0)$.

Auch hier kann ohne eine Zusatzvoraussetzung auf $k \equiv 1 \bmod. p$, also $\mu^T \underset{\mathfrak{p}}{=} \mu$ geschlossen werden. Es gilt hier nämlich [12])

$$\mu \underset{\mathfrak{p}}{\equiv} \pi^\nu \bmod. \mathfrak{p}^0 \quad \text{mit } \nu \not\equiv 0 \bmod. p,$$

wo $\pi = 1 - \zeta$ das Primelement zu $\mathfrak{p}$ in Z ist. Dann ist auch

$$\mu^T \underset{\mathfrak{p}}{\equiv} \pi^\nu \bmod. \mathfrak{p}^0,$$

da $\pi^T \underset{\mathfrak{p}}{\equiv} \pi \bmod. \mathfrak{p}^0$ (sogar $\bmod. \mathfrak{p}^1$) ist, während

$$\mu^k \underset{\mathfrak{p}}{\equiv} \pi^{k\nu} \bmod. \mathfrak{p}^0$$

ist. Aus $\mu^T \underset{\mathfrak{p}}{=} \mu^k$ folgt also hier

$$k\nu \equiv \nu \bmod. p,$$

wegen $\nu \not\equiv 0 \bmod. p$ also

$$k \equiv 1 \bmod. p \text{ [13])}.$$

Aus der damit in den drei Fällen $\alpha)$, $\beta)$, $\gamma)$ bestätigten Tatsache

$$\mu^T \underset{\mathfrak{p}}{=} \mu$$

folgt

$$N(\mu) = \mu^{1+T+\cdots+T^{p-2}} \underset{\mathfrak{p}}{=} \mu^{p-1} \underset{\mathfrak{p}}{=} \mu^{-1}.$$

Daher ist

$$\mathsf{N} = \mathsf{Z}(\sqrt[p]{\mu}) = \mathsf{Z}(\sqrt[p]{\mu^{-1}}) = \mathsf{Z}(\sqrt[p]{N(\mu)}) = \mathsf{P}(\zeta, \sqrt[p]{a})$$

mit rationalem $a = N(\mu)$, d. h. der Teilkörper p-ten Grades von N ist von der binomischen Form

$$\mathsf{K} = \mathsf{P}(\sqrt[p]{a}).$$

Damit ist der eingangs ausgesprochene Satz bewiesen.

---

[12]) Siehe H. Hasse, Bericht Ia, § 11.

[13]) Den Beweis für die Fälle $\beta)$ und $\gamma)$ stellte mir liebenswürdigerweise Herr Hasse zur Verfügung, wie schon in der Einleitung erwähnt wurde.

Zum Schluß soll noch gezeigt werden, daß

1. auflösbare Körper K vom Grade p über P existieren, deren Diskriminanten die im Satz im ersten Falle angegebene Gestalt haben, die aber nicht binomisch sind,

2. die im ersten Falle des Satzes gemachte Zusatzvoraussetzung über die Teilerfremdheit der Zahlen e_ν nicht auch notwendig für die Gültigkeit des Satzes ist,

3. die Zahl k, die als Exponent von μ bei Anwendung der Substitution T auftritt ($\mu^T \underset{p}{=} \mu^k$), eine einfache Bedeutung bei der Darstellung der Galoisschen Gruppe von N als Permutationsgruppe der Konjugierten des Teilkörpers p-ten Grades K hat.

1. Damit ein Kummerscher Körper $\mathsf{N} = \mathsf{Z}(\sqrt[p]{\mu}) = \mathsf{P}(\zeta, \sqrt[p]{\mu})$ über $\mathsf{Z} = \mathsf{P}(\zeta)$ ein Normalkörper über P mit der vollen linearen Gruppe als Galoisscher Gruppe und mit einem Führer $\mathfrak{f}_{\mathsf{N/Z}} = a_0$ (erster der obigen drei Fälle) ist, sind insgesamt folgende Bedingungen notwendig und hinreichend:

a) $\mu^T \underset{p}{=} \mu^k$ mit $(k, p) = 1$; dies ist notwendig und hinreichend dafür, daß $\mathsf{N/P}$ galoissch ist.

b) gk^{-1} ist mod. p von der Ordnung $p - 1$, wo g die aus $\zeta^T = \zeta^g$ bestimmte Primitivwurzel mod. p ist; dies ist notwendig und hinreichend dafür, daß $\mathsf{N/P}$ die volle lineare Gruppe als Galoissche Gruppe hat.

c) $\mu \underset{p}{\equiv} 1$ mod. $p\mathfrak{p}$, wo $(p) = \mathfrak{p}^p$ in Z; dies ist notwendig und hinreichend dafür, daß $\mathfrak{p}$ nicht in $\mathfrak{f}_{\mathsf{N/Z}}$ vorkommt.

d) μ enthält nur Primteiler der $p_\nu \mid a_0$ zu durch p unteilbaren Exponenten, und für jedes p_ν wirklich mindestens einen solchen; dies ist notwendig und hinreichend dafür, daß $\mathfrak{f}_{\mathsf{N/Z}} = a_0$ ist.

Ist der in a) auftretende Exponent $k \equiv 1$ mod. p, so ist der in N enthaltene Teilkörper p-ten Grades K nach dem Schluß unseres obigen Beweises binomisch (und zwar fällt er unter den ersten Fall unseres Satzes, wegen $\mathfrak{f}_{\mathsf{N/Z}} = a_0$). Ist umgekehrt $\mathsf{K} = \mathsf{P}(\sqrt[p]{a})$ binomisch, so hat man

$$\mu \underset{p}{=} a^\varkappa \quad \text{mit } (\varkappa, p) = 1$$

und daher

$$\mu^T \underset{p}{=} \mu,$$

d. h. $k \equiv 1$ mod. p. Wir haben also in

e) $k \not\equiv 1$ mod. p

die notwendige und hinreichende Bedingung dafür, daß für einen Kummerschen Körper N mit den Eigenschaften a)—d) der Teilkörper p-ten Grades K nicht binomisch ist.

Ich gebe zunächst eine spezielle Realisierung der Bedingungen a)—e). Es sei $p = 5$, also etwa $g = 2$, $\zeta^T = \zeta^2$. Dann nehme ich

$$\mu = \alpha^{1+4T+T^3+4T^3} \quad \text{mit } \alpha = 5\zeta - 4,$$

also ausführlicher

$$\mu = (5\zeta - 4)\ (5\zeta^2 - 4)^4\ (5\zeta^4 - 4)\ (5\zeta^2 - 4)^4.$$

Ersichtlich ist

$$\mu^T \underset{p}{=} \mu^4,$$

d. h. a) und e) sind mit $k \equiv 4$ mod. 5 erfüllt. Da $gk^{-1} \equiv 3$ mod. 5 ist, ist auch b) erfüllt.

Ferner ist ersichtlich

$$\alpha = 5\zeta - 4 \equiv 5 \cdot 1 - 4 \equiv 1 \bmod. 5\mathfrak{p}$$

und dann auch $\alpha^{T^\nu} \equiv 1 \bmod. 5\mathfrak{p}$, also

$$\mu \equiv 1 \bmod. 5\mathfrak{p},$$

d. h. c) ist erfüllt. Schließlich hat man die Zerlegung

$$\alpha = 5\zeta - 4 = (\zeta^3 + 2\zeta)\ (4 + 2\zeta + \zeta^3)$$

mit

$$N(\zeta^3 + 2\zeta) = 11, \quad N(4 + 2\zeta + \zeta^3) = 191,$$

so daß also (α) Produkt zweier Primhauptideale ersten Grades

$$\mathfrak{p}_1 = (\zeta^3 + 2\zeta), \quad \mathfrak{p}_2 = (4 + 2\zeta + \zeta^3)$$

mit

$$N(\mathfrak{p}_1) = 11, \quad N(\mathfrak{p}_2) = 191$$

ist, und daher

$$(\mu) = (\mathfrak{p}_1 \mathfrak{p}_2)^{1+4T+T^2+4T^3}.$$

Daher ist d) mit $p_1 = 11$, $p_2 = 191$ erfüllt.

Herr Hasse teilte mir freundlicherweise mit, wie man die obigen Bedingungen a)—e) in allgemeinerer Weise realisieren kann. Sei p eine solche Primzahl, daß der p-te Kreisteilungskörper Z eine genau durch p^1 teilbare Klassenanzahl hat, während jeder Teilkörper von Z eine durch p unteilbare Klassenzahl hat (z. B. $p = 59$). Dann hat der p-Klassenkörper N von Z die Eigenschaften a)—d). Denn N ist seiner invarianten Definition nach galoissch über P, ferner unter den gemachten Annahmen zyklisch vom Grade p über Z und besitzt keinen Teilkörper, der über einem Teilkörper von Z zyklisch vom Grade p ist, d. h. N hat die volle lineare Gruppe als Galoissche Gruppe, und schließlich ist N unverzweigt über Z, also $\mathfrak{f}_{N/Z} = 1$. Wegen $\mathfrak{f}_{N/Z} = 1$ hat der in N enthaltene Teilkörper p-ten Grades K die Diskriminante $\vartheta_{K/P} = \vartheta_{N/Z} = p^{p-2}$, ist also nach dem auf S. 2 Gesagten sicher nicht binomisch.

Ich will noch zeigen, daß sich die Bedingungen a)—e) auch mit $\mathfrak{f}_{N/Z} \neq 1$ realisieren lassen, sogar mit beliebig vielen Primteilern p_ν von $\mathfrak{f}_{N/Z}$. Sei dazu $k \not\equiv 1 \bmod. p$ vorgegeben und e ein Exponent mit

$$k^e \equiv 1 \bmod. p, \ ef = p - 1$$

(nicht notwendig der genaue Exponent von k mod. p). Ferner seien die p_ν irgendwelche Primzahlen $(\neq 2)$, die mod. p vom genauen Exponenten f sind. Sei dann Z_e der Teilkörper e-ten Grades von Z, also der Zerlegungskörper für die Primzahlen p_ν im Körper Z, und sei jeweils $\mathfrak{p}_\nu$ ein Primteiler von p_ν in Z, der dann schon Primideal (ersten Grades) in Z_e ist. Wir wählen dann Zahlen γ_ν in Z_e mit den Eigenschaften:

γ_ν ist genau durch $\mathfrak{p}_\nu^1$ teilbar,

γ_ν ist prim zu den Konjugierten $\mathfrak{p}_\nu^T, \ldots, \mathfrak{p}_\nu^{T^{e-1}}$,

γ_ν ist prim zu den $p_{\nu'} (\nu' \neq \nu)$,

$\gamma_\nu \underset{p}{\equiv} 1 \bmod. p\mathfrak{p}$.

Solche γ_ν existieren bekanntlich stets. Damit bilden wir die symbolischen Potenzen

$$\eta_\nu \underset{p}{=} \gamma_\nu^{1+k^{-1}T+\cdots+k^{-(e-1)}T^{e-1}},$$

wo im Exponenten mod. p gerechnet sei, und damit das Produkt

$$\mu \underset{p}{=} \prod_{\nu} \eta_\nu .$$

Dieses μ hat dann, wie leicht aus der Konstruktion ersichtlich ist, die Eigenschaften a)—e), mit durch die gewählten p_ν teilbarem $\mathfrak{f}_{N/Z}$.

2. Ich zeige, daß die im ersten der drei Fälle des Satzes gemachte Annahme, daß die Zahlen e_ν teilerfremd sind, nicht notwendig dafür ist, daß zu vorgegebener Diskriminante $\vartheta_{K/P} = p^{p-2} a_0^{p-1}$ nur binomische Körper existieren, indem ich ein Beispiel mit $a_0 = p_1$, $e_1 = 2$ konstruiere, in dem zur Diskriminante $\vartheta_{K/P} = p^{p-2} p_1^{p-1}$ nur der binomische Körper $K = P(\sqrt[p]{p_1})$ gehört.

Sei dazu $p = 7$, also etwa $g = 3$, und ferner $p_1 = 67$, also $f_1 = 3$, $e_1 = 2$, wegen $67^3 \equiv 1 \bmod. 7$. Der binomische Körper $K = P(\sqrt[7]{67})$ fällt wegen $67 \equiv 18 \bmod. 7^2$ und $18^6 \equiv 1 \bmod. 7^2$ (Jacobi!), also $67^6 \equiv 1 \bmod. 7^2$ unter den ersten Fall des Satzes, hat also die Diskriminante $\vartheta_{K/P} = 7^5 \cdot 67^6$. Andrerseits ergeben die obigen Bedingungen b) und e) für einen nicht binomischen auflösbaren Körper 7-ten Grades dieser Diskriminante notwendig $k \equiv 2 \bmod. 7$, so daß also $k^{e_1} \equiv 2^2 \not\equiv 1 \bmod. 7$ wäre, während doch im Beweis auf S. 8 allgemein $k^{e_\nu} \equiv 1 \bmod. p$ festgestellt wurde. Daher gibt es außer $K = P(\sqrt[7]{67})$ keinen auflösbaren Körper 7-ten Grades mit der Diskriminante $7^5 \cdot 67^6$.

3. Ich will noch eine einfache gruppentheoretische Bestimmung der Zahl k geben, die einem über P galoisschen Körper $N = P(\zeta, \sqrt[p]{\mu})$ mit der vollen linearen Gruppe als Galoisscher Gruppe $\mathfrak{G}$ durch die Relation $\mu^T \underset{p}{=} \mu^k$ invariant zugeordnet ist. $\mathfrak{G}$ wird erzeugt durch

$$S = \begin{pmatrix} \zeta & : & \zeta \\ \sqrt[p]{\mu} & : & \zeta\sqrt[p]{\mu} \end{pmatrix} \quad \text{und} \quad T = \begin{pmatrix} \zeta & : & \zeta \\ \sqrt[p]{\mu} & : & \sqrt[p]{\mu^k \gamma} \end{pmatrix},$$

mit den Relationen

$$S^p = T^{p-1} = E \quad \text{und} \quad ST = TS^r .$$

Dabei sind g und r Primitivwurzeln mod. p, und γ ist die in der Relation $\mu^T = \mu^k \gamma^p$ auftretende Zahl aus Z. Durch Anwendung von $ST = TS^r$ auf die Zahl $\sqrt[p]{\mu}$ ergibt sich

$$g \equiv kr \bmod. p,$$

also insbesondere die oben angeführte Bedingung b), daß gk^{-1} mod. p von der Ordnung $p - 1$ ist. Sei nun der Teilkörper p-ten Grades K unter seinen Konjugierten als der Invariantenkörper von T festgelegt, ferner sei $K = P(\alpha)$ irgendeine Erzeugung von K, und seien die Konjugierten $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$ von α gruppentheoretisch durch $\alpha_\nu = \alpha^{S^\nu}$ (ν mod. p) festgelegt. Dann stellt sich $\mathfrak{G}$ als die volle lineare Permutationsgruppe der p Konjugierten α_ν dar, und zwar

$$S \text{ als der } p\text{-gliedrige Zyklus } \begin{pmatrix} \alpha_\nu \\ \alpha_{\nu+1} \end{pmatrix},$$

$$T \text{ als der } (p-1)\text{-gliedrige Zyklus } \begin{pmatrix} \alpha_\nu \\ \alpha_{\nu r} \end{pmatrix}.$$

Geht man von $K = P(\alpha)$ aus, und sind $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$ die Konjugierten zu α in solcher Reihenfolge, daß die eben genannten beiden zyklischen Permutationen die

Galoissche Gruppe $\mathfrak{G}$ erzeugen, so bestimmt sich die zu der hierbei willkürlich gewählten Primitivwurzel r im Sinne des Vorhergehenden gehörige Primitivwurzel g auf Grund der Tatsache

$$\mathsf{N} = \mathsf{P}(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) \geqq \mathsf{Z} = \mathsf{P}(\zeta),$$

indem man eine rationale Darstellung von ζ durch die α_ν aufsucht:

$$f(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) = \zeta^\varrho,$$

und darin die Permutation $\begin{pmatrix} \alpha_\nu \\ \alpha_{\nu r} \end{pmatrix}$ anwendet:

$$f(\alpha_0, \alpha_r, \ldots, \alpha_{(p-1)r}) = \zeta^\varrho.$$

Daraus bestimmt sich dann die Invariante k gemäß der obigen Relation

$$g \equiv kr \bmod. p.$$

Eingegangen 23. April 1936.

wo im Exponenten mod. p gerechnet sei, und damit das Produkt

$$\mu \underset{p}{=} \prod_{\nu} \eta_\nu .$$

Dieses μ hat dann, wie leicht aus der Konstruktion ersichtlich ist, die Eigenschaften a)—e), mit durch die gewählten p_ν teilbarem $\mathfrak{f}_{N/Z}$.

2. Ich zeige, daß die im ersten der drei Fälle des Satzes gemachte Annahme, daß die Zahlen e_ν teilerfremd sind, nicht notwendig dafür ist, daß zu vorgegebener Diskriminante $\vartheta_{K/P} = p^{p-2} a_0^{p-1}$ nur binomische Körper existieren, indem ich ein Beispiel mit $a_0 = p_1$, $e_1 = 2$ konstruiere, in dem zur Diskriminante $\vartheta_{K/P} = p^{p-2} p_1^{p-1}$ nur der binomische Körper $K = P(\sqrt[p]{p_1})$ gehört.

Sei dazu $p = 7$, also etwa $g = 3$, und ferner $p_1 = 67$, also $f_1 = 3$, $e_1 = 2$, wegen $67^3 \equiv 1 \bmod. 7$. Der binomische Körper $K = P(\sqrt[7]{67})$ fällt wegen $67 \equiv 18 \bmod. 7^2$ und $18^6 \equiv 1 \bmod. 7^2$ (Jacobi!), also $67^6 \equiv 1 \bmod. 7^2$ unter den ersten Fall des Satzes, hat also die Diskriminante $\vartheta_{K/P} = 7^5 \cdot 67^6$. Andrerseits ergeben die obigen Bedingungen b) und e) für einen nicht binomischen auflösbaren Körper 7-ten Grades dieser Diskriminante notwendig $k \equiv 2 \bmod. 7$, so daß also $k^{e_1} \equiv 2^2 \not\equiv 1 \bmod. 7$ wäre, während doch im Beweis auf S. 8 allgemein $k^{e_\nu} \equiv 1 \bmod. p$ festgestellt wurde. Daher gibt es außer $K = P(\sqrt[7]{67})$ keinen auflösbaren Körper 7-ten Grades mit der Diskriminante $7^5 \cdot 67^6$.

3. Ich will noch eine einfache gruppentheoretische Bestimmung der Zahl k geben, die einem über P galoisschen Körper $N = P(\zeta, \sqrt[p]{\mu})$ mit der vollen linearen Gruppe als Galoisscher Gruppe $\mathfrak{G}$ durch die Relation $\mu^T \underset{p}{=} \mu^k$ invariant zugeordnet ist. $\mathfrak{G}$ wird erzeugt durch

$$S = \begin{pmatrix} \zeta & : & \zeta \\ \sqrt[p]{\mu} & : & \zeta\sqrt[p]{\mu} \end{pmatrix} \quad \text{und} \quad T = \begin{pmatrix} \zeta & : & \zeta \\ \sqrt[p]{\mu} & : & \sqrt[p]{\mu^k \gamma} \end{pmatrix},$$

mit den Relationen

$$S^p = T^{p-1} = E \quad \text{und} \quad ST = TS^r .$$

Dabei sind g und r Primitivwurzeln mod. p, und γ ist die in der Relation $\mu^T = \mu^k \gamma^p$ auftretende Zahl aus Z. Durch Anwendung von $ST = TS^r$ auf die Zahl $\sqrt[p]{\mu}$ ergibt sich

$$g \equiv kr \bmod. p,$$

also insbesondere die oben angeführte Bedingung b), daß gk^{-1} mod. p von der Ordnung $p - 1$ ist. Sei nun der Teilkörper p-ten Grades K unter seinen Konjugierten als der Invariantenkörper von T festgelegt, ferner sei $K = P(\alpha)$ irgendeine Erzeugung von K, und seien die Konjugierten $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$ von α gruppentheoretisch durch $\alpha_\nu = \alpha^{S^\nu}$ (ν mod. p) festgelegt. Dann stellt sich $\mathfrak{G}$ als die volle lineare Permutationsgruppe der p Konjugierten α_ν dar, und zwar

$$S \text{ als der } p\text{-gliedrige Zyklus } \begin{pmatrix} \alpha_\nu \\ \alpha_{\nu+1} \end{pmatrix},$$

$$T \text{ als der } (p-1)\text{-gliedrige Zyklus } \begin{pmatrix} \alpha_\nu \\ \alpha_{\nu r} \end{pmatrix}.$$

Geht man von $K = P(\alpha)$ aus, und sind $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$ die Konjugierten zu α in solcher Reihenfolge, daß die eben genannten beiden zyklischen Permutationen die

Galoissche Gruppe $\mathfrak{G}$ erzeugen, so bestimmt sich die zu der hierbei willkürlich gewählten Primitivwurzel r im Sinne des Vorhergehenden gehörige Primitivwurzel g auf Grund der Tatsache

$$\mathsf{N} = \mathsf{P}(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) \geqq \mathsf{Z} = \mathsf{P}(\zeta),$$

indem man eine rationale Darstellung von ζ durch die α_ν aufsucht:

$$f(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) = \zeta^\vartheta,$$

und darin die Permutation $\begin{pmatrix} \alpha_\nu \\ \alpha_{\nu r} \end{pmatrix}$ anwendet:

$$f(\alpha_0, \alpha_r, \ldots, \alpha_{(p-1)r}) = \zeta^\vartheta.$$

Daraus bestimmt sich dann die Invariante k gemäß der obigen Relation

$$g \equiv kr \bmod. p.$$

Eingegangen 23. April 1936.

Über die Diskriminante auflösbarer Körper von Primzahlgrad.

Von *Helmut Hasse* in Göttingen.

Für die Diskriminante eines über dem rationalen Zahlkörper P kubischen Körpers K gilt bekanntlich [1]) die Formel

$$D = df^2,$$

wo d die Diskriminante des im galoisschen Körper N zu K enthaltenen quadratischen Teilkörpers Z ist (falls schon $K = N$ galoissch ist, ist $Z = P$, $d = 1$ zu rechnen) und f der Führer des kubisch-zyklischen Relativkörpers N/Z. Dieser Tatbestand wurde von Wegner [2]) und Porusch [3]) auf beliebige auflösbare Körper K vom Primzahlgrad p über dem rationalen Zahlkörper verallgemeinert. Hier ist die Diskriminante (als Ideal, also abgesehen vom Vorzeichen) durch die Formel

$$\mathfrak{D}_{K/P} = \mathfrak{D}_{Z/P}^{\frac{p-1}{n}} \cdot \mathfrak{f}_{N/Z}^{p-1}$$

gegeben, wo wieder N der galoissche Körper zu K ist, der dann zyklisch von einem Grade $n | p-1$ über K ist, und ferner zyklisch vom Grade p über einem über P vom Grade n zyklischen Teilkörper Z.

Diese für den Aufbau der Arithmetik in K wichtige Diskriminantenformel wurde von Wegner auf analytischem Wege, durch Vergleich von Zetafunktionalgleichungen, bewiesen. Porusch führt den Beweis in begrifflich nicht sehr befriedigender Weise folgendermaßen: Er stellt alle gruppentheoretisch möglichen Typen für die Hilbertsche Untergruppenreihe zu einer Primzahl q für N/P tabellarisch auf, gibt dabei jeweils die q-Beiträge zu den einzelnen Teilkörperdiskrimianten und Führern an, und liest so für die einzelnen q-Beiträge die Gültigkeit der fraglichen Formel ab.

Ich will hier zeigen, wie man diese Diskriminantenformel in einfacher Weise aus der von Artin [4]) entwickelten gruppentheoretischen Strukturtheorie der Diskriminante herleiten kann, die als formal-algebraisches Gerüst hinter der Wegnerschen analytischen Schlußweise steckt. Anschließend gebe ich noch einige Folgerungen, die im Zusammenhang mit der vorstehenden Arbeit von Wegner stehen.

1.

Sei Ω ein beliebiger algebraischer Zahlkörper, K ein über Ω auflösbarer Körper vom Primzahlgrad p, N der zugehörige galoissche Körper über Ω. Dann ist die Galois-

[1]) Siehe etwa H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, Math. Zeitschr. **31** (1930), 575, Satz 3 und 4.

[2]) U. Wegner, Zur Theorie der auflösbaren Gleichungen von Primzahlgrad. I, Journ. f. Math. **168** (1932), 183.

[3]) I. Porusch, Die Arithmetik in Zahlkörpern, deren zugehörige galoissche Körper spezielle metabelsche Gruppen besitzen, auf klassenkörpertheoretischer Grundlage, Math. Zeitschr. **37** (1933), 149, Satz VII.

[4]) E. Artin, Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper, Journ. f. Math. **164** (1931), 1—11. — Im folgenden zitiert mit „Artin".

gruppe $\mathfrak{G}$ von N/Ω bekanntlich von der Struktur:

$$S^p = 1, \quad T^n = 1, \quad TST^{-1} = S^r,$$

wobei n ein Teiler von $p-1$ und r eine Restklasse mod. p von der Ordnung n ist. K ist der Invariantenkörper etwa der Untergruppe $\{T\}$; der Invariantenkörper Z des Normalteilers $\{S\}$ ist zyklisch vom Grade n über Ω, sowie N zyklisch vom Grade p über Z.

Zur Anwendung der Artinschen Theorie haben wir zunächst die absolut-irreduziblen Darstellungen von $\mathfrak{G}$ aufzustellen. Wir geben die Darstellungsmatrizen selbst nur für die Erzeugenden S und T von $\mathfrak{G}$ an, und berechnen daraus die Charaktere der Darstellungen jeweils für die drei Typen von Elementen:

$$1, \quad S^i \quad (i = 1, \ldots, p-1), \quad S^i T^j \quad \begin{pmatrix} i = 0, 1, \ldots, p-1 \\ j = 1, 2, \ldots, n-1 \end{pmatrix}.$$

a) Die n Darstellungen ersten Grades der zyklischen Faktorgruppe $\mathfrak{G}/\{S\} \cong \{T\}$ liefern n Darstellungen ersten Grades auch für $\mathfrak{G}$:

$$S \to 1, \quad T \to \varepsilon^\nu \qquad (\nu = 0, 1, \ldots, n-1)$$

(ε primitive n-te Einheitswurzel),

mit den Charakteren

$$\psi_\nu(1) = 1, \quad \psi_\nu(S^i) = 1, \quad \psi_\nu(S^i T^j) = \varepsilon^{j\nu}.$$

b) Weitere Darstellungen ergeben sich, indem man von einer (nicht-identischen) Darstellung ersten Grades der Untergruppe $\{S\}$ ausgeht:

$$S \to \zeta^\mu \qquad (\mu \not\equiv 0 \bmod. p)$$

(ζ primitive p-te Einheitswurzel),

mit dem Charakter

$$\varphi_\mu(1) = 1, \quad \varphi_\mu(S^i) = \zeta^{i\mu},$$

und die zugehörige induzierte Darstellung von $\mathfrak{G}$ bildet. Entsprechend den Relationen

$$T^\nu \cdot S = S^{r^\nu} T^\nu, \quad T^\nu \cdot T = T^{\nu+1} \qquad (\nu = 0, 1, \ldots, n-1)$$

ergibt sich als induzierte Darstellung

$$S \to \begin{pmatrix} \zeta^\mu & & & \\ & \zeta^{\mu r} & & \\ & & \ddots & \\ & & & \zeta^{\mu r^{n-1}} \end{pmatrix}, \quad T \to \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{pmatrix},$$

mit dem Charakter

$$\chi_{\varphi_\mu}(1) = n, \qquad \chi_{\varphi_\mu}(S^i) = \sum_{\nu=0}^{n-1} \zeta^{i\mu r^\nu} = \eta_{i\mu}, \qquad \chi_{\varphi_\mu}(S^i T^j) = 0$$

(p-te Kreisteilungsperioden m-ten Grades).

Dabei kommt es auf μ nur mod. $\{r\}$, der durch r erzeugten Untergruppe der Ordnung n der primen Restklassengruppe mod. p, an; es genügt also, μ ein volles Repräsentantensystem von $m = \dfrac{p-1}{n}$ Resten mod. p nach dieser Untergruppe $\{r\}$ durchlaufen zu lassen. Im folgenden habe μ durchweg diese Bedeutung.

So entstehen m wegen der Verschiedenheit ihrer Charaktere nicht-äquivalente Darstellungen n-ten Grades von G. Der zugehörige Gruppenring über dem Körper $\mathsf{P}(\eta)$ des Charakters (Körper der p-ten Kreisteilungsperioden m-ten Grades) ist jedesmal das zyklische verschränkte Produkt des p-ten Kreiskörpers $\mathsf{P}(\xi)/\mathsf{P}(\eta)$ mit Faktorensystem 1,

also eine einfache normale Algebra vom Grade n über $\mathsf{P}(\eta)$; daher sind die erhaltenen m Darstellungen n-ten Grades absolut-irreduzibel.

Die damit gewonnenen $n + m$ nicht-äquivalenten absolut-irreduziblen Darstellungen von G sind bereits ein vollständiges System. Denn die Quadratsumme ihrer Grade ergibt

$$n \cdot 1^2 + m \cdot n^2 = n + \frac{p-1}{n} n^2 = n + (p-1)n = pn,$$

also die Ordnung von $\mathfrak{G}$.

2.

Nach Artin (20) ist die Diskriminante von K/Ω gegeben durch

$$\mathfrak{D}_{\mathsf{K}/\Omega} = \mathfrak{f}(\chi_{\psi_0^0},\ \mathsf{N}/\Omega),$$

wo ψ_0^0 die identische Darstellung der K zugeordneten Untergruppe $\{T\}$ bezeichnet. Zur Berechnung des Führers rechts haben wir die durch ψ_0^0 induzierte Darstellung von $\mathfrak{G}$ in ihre absolut-irreduziblen Bestandteile zu zerlegen. Diese induzierte Darstellung ist nun, entsprechend den Relationen

$$S \cdot S^k = S^{k+1}, \qquad T \cdot S^k = S^{kr} T,$$

die bekannte Darstellung von $\mathfrak{G}$ als lineare Permutationsgruppe p-ten Grades mod. p, mit dem Charakter

$$\chi_{\psi_0^0}(1) = p, \qquad \chi_{\psi_0^0}(S^i) = 0, \qquad \chi_{\psi_0^0}(S^i T^j) = 1.$$

Andrerseits liefert auch die aus den oben bestimmten absolut-irreduziblen Charakteren gebildete Summe $\psi_0 + \sum_\mu \chi_{\varphi_\mu}$ die Werte

$$\psi_0(1) + \sum_\mu \chi_{\varphi_\mu}(1) = 1 + mn = p, \quad \psi_0(S^i) + \sum_\mu \chi_{\varphi_\mu}(S^i) = 1 + \sum_\mu \eta_{i\mu} = 0, \quad \psi_0(S^i T^j) + \sum_\mu \chi_{\varphi_\mu}(S^i T^j) = 1 + 0 = 1.$$

Somit gilt

$$\chi_{\psi_0^0} = \psi_0 + \sum_\mu \chi_{\varphi_\mu}.$$

Daraus folgt nach Artin (18)

$$\mathfrak{D}_{\mathsf{K}/\Omega} = \mathfrak{f}(\chi_{\psi_0^0},\ \mathsf{N}/\Omega) = \mathfrak{f}(\psi_0,\ \mathsf{N}/\Omega) \cdot \prod_\mu \mathfrak{f}(\chi_{\varphi_\mu},\ \mathsf{N}/\Omega) = \prod_\mu \mathfrak{f}(\chi_{\varphi_\mu},\ \mathsf{N}/\Omega),$$

letzteres, da für den Hauptcharakter ψ_0 von $\mathfrak{G}$ gilt

$$\mathfrak{f}(\psi_0,\ \mathsf{N}/\Omega) = 1.$$

Ferner ist nach Artin (19)

$$\mathfrak{f}(\chi_{\varphi_\mu},\ \mathsf{N}/\Omega) = \mathfrak{D}_{\mathsf{Z}/\Omega} \cdot N_{\mathsf{Z}/\Omega}(\mathfrak{f}(\varphi_\mu,\ \mathsf{N}/\mathsf{Z})),$$

also

$$\mathfrak{D}_{\mathsf{K}/\Omega} = \mathfrak{D}_{\mathsf{Z}/\Omega}^m \cdot \prod_\mu N_{\mathsf{Z}/\Omega}(\mathfrak{f}(\varphi_\mu,\ \mathsf{N}/\mathsf{Z})).$$

Weil konjugiert-algebraische Charaktere denselben Führer haben, sind alle $\mathfrak{f}(\varphi_\mu,\ \mathsf{N}/\mathsf{Z})$ einander gleich, und ihr gemeinsamer Wert $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}}$ ist bei den Automorphismen von Z/Ω invariant. Wir haben somit schließlich

$$(1) \qquad \mathfrak{D}_{\mathsf{K}/\Omega} = \mathfrak{D}_{\mathsf{Z}/\Omega}^m \cdot N_{\mathsf{Z}/\Omega}(\mathfrak{f}_{\mathsf{N}/\mathsf{Z}})^m = \mathfrak{D}_{\mathsf{Z}/\Omega}^{\frac{p-1}{n}} \cdot \mathfrak{f}_{\mathsf{N}/\mathsf{Z}}^{p-1}.$$

Damit ist die eingangs angeführte Wegner-Poruschsche Diskriminantenformel (für einen beliebigen Grundkörper Ω statt P) bewiesen, und zwar auf formal-gruppen-

theoretischem Wege, ohne die klassenkörpertheoretische Bedeutung von $f_{N/Z}$ als Führer der N in Z zugeordneten Idealgruppe $H_{N/Z}$ heranzuziehen.

Auch die aus der Klassenkörpertheorie bekannte Formel

$$\mathfrak{D}_{N/Z} = f_{N/Z}^{p-1} \tag{2}$$

ergibt sich ohne weiteres auf diesem formal-gruppentheoretischen Wege, ebenso die bekannte Relativdiskriminantenformel

$$\mathfrak{D}_{N/\Omega} = \mathfrak{D}_{Z/\Omega}^{p} \cdot N_{Z/\Omega}(\mathfrak{D}_{N/Z}) = \mathfrak{D}_{Z/\Omega}^{p} \cdot \mathfrak{f}_{N/Z}^{n(p-1)} . \tag{3}$$

Durch Kombination mit der obigen Diskriminantenformel (1) ergibt sich aus ihr die von Wegner in der vorstehenden Arbeit benutzte Formel

$$\mathfrak{D}_{N/\Omega} = \mathfrak{D}_{Z/\Omega} \cdot \mathfrak{D}_{K/\Omega}^{n} . \tag{4}$$

3.

Porusch hat (im Spezialfall $\Omega = P$) noch die folgende Tatsache aus seiner tabellarischen Zusammenstellung abgelesen (a. a. O. 149, Satz VI):

$\mathfrak{D}_{Z/\Omega}$ *und* $\mathfrak{f}_{N/Z}$ *haben höchstens Primteiler von* p *gemeinsam.*

Dies läßt sich ganz einfach mittels der Diskriminantenformeln (1) und (4) beweisen. Aus Teilbarkeitsgründen für die Verzweigungsordnungen ist ohne weiteres klar:

Ein Primideal $\mathfrak{q}_\Omega$ ist dann und nur dann voll-verzweigt in K ($\mathfrak{q}_\Omega = \mathfrak{q}_K^p$), wenn einer (und damit jeder) seiner Primteiler $\mathfrak{q}_Z$ verzweigt in N ist ($\mathfrak{q}_Z = \mathfrak{q}_N^p$).

Sei nun $\mathfrak{q}_Z \mid \mathfrak{f}_{N/Z}$, also $\mathfrak{q}_Z = \mathfrak{q}_N^p$, und somit $\mathfrak{q}_\Omega = \mathfrak{q}_K^p$, so ist für $\mathfrak{q}_\Omega \neq p$ nach dem Dedekindschen Diskriminantensatz der Beitrag

$$\mathfrak{D}_{K/\Omega}(\mathfrak{q}_\Omega) = \mathfrak{q}_\Omega^{p-1} .$$

Da für $\mathfrak{q}_\Omega \neq p$ in N/Z keine höhere Verzweigung vorliegt, ist ferner etwa nach Artin (17),

$$\mathfrak{f}_{N/Z}(\mathfrak{q}_\Omega) = \mathfrak{q}_\Omega^{\frac{1}{e}} ,$$

wo e die Verzweigungsordnung für Z/Ω ist, also

$$\mathfrak{f}_{N/Z}(\mathfrak{q}_\Omega)^{p-1} = \mathfrak{q}_\Omega^{\frac{p-1}{e}} .$$

Nach der Diskriminantenformel (1) ist daher

$$\mathfrak{D}_{Z/\Omega}(\mathfrak{q}_\Omega) = \mathfrak{q}_\Omega^{n\left(1-\frac{1}{e}\right)} ,$$

und weiter nach (4)

$$\mathfrak{D}_{N/\Omega}(\mathfrak{q}_\Omega) = \mathfrak{q}_\Omega^{n\left(1-\frac{1}{e}\right)+n(p-1)} = \mathfrak{q}_\Omega^{np\left(1-\frac{1}{ep}\right)} .$$

Da ep die Verzweigungsordnung für N/Ω ist, liegt also gemäß dem Dedekindschen Diskriminantensatz auch für Z/Ω und N/Ω keine höhere Verzweigung vor, d. h. die Trägheitsgruppe für N/Ω ist zyklisch von der Ordnung ep. Mit Hinblick auf die Struktur der Gruppe $\mathfrak{G}$ ist dies nur für $e = 1$ möglich, und das bedeutet $\mathfrak{q}_\Omega \neq \mathfrak{D}_{Z/\Omega}$.

4.

Sei von jetzt an der Grundkörper $\Omega = P$. Spezielle Körper K der betrachteten Art sind die binomischen Körper

$$K = P(\sqrt[p]{a}) ,$$

wo a eine Zahl aus P ist, die keine p-te Potenz in P ist, und die ganz und p-te-potenzfrei angenommen werden kann. Für diese Körper K ist

$$\mathsf{N} = \mathsf{P}(\zeta, \sqrt[p]{a}), \quad \mathsf{Z} = \mathsf{P}(\zeta), \quad n = p - 1 .$$

Ferner ist

$$p = \mathfrak{p}^{p-1}, \quad \mathfrak{p} = (1 - \zeta)$$

in Z, und

$$\mathfrak{D}_{\mathsf{Z/P}} = p^{p-2} .$$

Nach der Theorie der Kummerschen Körper ist, wenn a_0 das Produkt der von p und untereinander verschiedenen Primzahlen $q \mid a$ bezeichnet,

$$\mathfrak{f}_{\mathsf{N/Z}} = \begin{cases} \mathfrak{p}^0 \; a_0, & \text{wenn} \quad p \nmid a, \quad a^{p-1} \equiv 1 \bmod. p^2 \\ \mathfrak{p}^2 \; a_0, & \text{wenn} \quad p \nmid a, \quad a^{p-1} \not\equiv 1 \bmod. p^2 \\ \mathfrak{p}^{p+1} a_0, & \text{wenn} \quad p \mid a \end{cases} .$$

Nach (1) ist also entsprechend

$$\mathfrak{D}_{\mathsf{K/P}} = p^{p-2} \begin{Bmatrix} p^0 & a_0^{p-1} \\ p^2 & a_0^{p-1} \\ p^{p+1} & a_0^{p-1} \end{Bmatrix}, \tag{5}$$

wie es von Wegner a. a. O. 182 festgestellt wurde.

5.

Sei jetzt umgekehrt, wie in der vorstehenden Arbeit von Wegner, vorausgesetzt, daß K ein auflösbarer Körper vom Primzahlgrad p über P ist, dessen Diskriminante $\mathfrak{D}_{\mathsf{K/P}}$ von einer der drei Formen (5) ist, wo jetzt $a_0 = q_1 \cdots q_s$ ein gegebenes Produkt untereinander und von p verschiedener Primzahlen ist.

Wegner findet dann die folgenden Bedingungen als hinreichend dafür, daß K binomisch über P ist:

Die Primzahl 2 kommt nicht unter den q_i vor.

Bei Vorliegen der ersten Form von $\mathfrak{D}_{\mathsf{K/P}}$ in (5) ist $s \geqq 1$, und wenn f_i die Ordnungen der q_i mod. p sind, so sind die Zahlen

$$e_i = \frac{p-1}{f_i}$$

teilerfremd.

Ich will hier nur noch zeigen, wie man die folgenden drei vorbereitenden Feststellungen für Wegners Beweis unmittelbar aus der Diskriminnatenformel (1) ablesen kann:

a) Es ist $n = p - 1$.

b) Es ist $p = \mathfrak{p}^{p-1}$ in Z.

c) Es ist $\mathfrak{f}_{\mathsf{Z/P}} = p$ oder $4p$, je nachdem $2 \nmid \mathfrak{D}_{\mathsf{Z/P}}$ oder $2 \mid \mathfrak{D}_{\mathsf{Z/P}}$.

Ad a). Vergleicht man die Voraussetzung (5) mit der Diskriminantenformel (1) (erste Form) und beachtet, daß p in (5) einen Exponenten $\equiv \pm 1$ mod. p hat, so ergibt sich $m \mid 1$, also $m = 1$, d. h. $n = p - 1$.

Ad b). Bezeichnet e die Verzweigungsordnung von p für $\mathsf{Z/P}$, so ist nach dem Dedekindschen Diskriminantensatz

$$\mathfrak{D}_{\mathsf{Z/P}}(p) = p^{(p-1)\left(1-\frac{1}{e}\right)} .$$

Ferner ist, etwa nach Artin (17),

$$\mathfrak{f}_{N/Z}(p) = p^{\frac{1}{e}(v+1)},$$

wo v die Anzahl der von 1 verschiedenen Verzweigungsgruppen für N/Z ist. Nach der Diskriminantenformel (1) ist also

$$\mathfrak{D}_{K/P}(p) = p^{(p-1)\left(1-\frac{1}{e}+\frac{v+1}{e}\right)} = p^{p-1+\frac{p-1}{e}v}.$$

Vergleicht man dies mit der Voraussetzung (5), so folgt

$$\frac{p-1}{e}\,v = \left\{\begin{matrix} -1 \\ 1 \\ p \end{matrix}\right\},$$

also notwendig $\dfrac{p-1}{e} = 1$, d. h. $e = p-1$.

Ad c). Angenommen $\mathfrak{D}_{Z/P}$ enthält außer p noch eine andere Primzahl q. Nach dem oben Gezeigten gehen dann die $\mathfrak{q}_Z$ nicht in $\mathfrak{f}_{N/Z}$ auf, so daß also nach (1) und (5)

$$\mathfrak{D}_{Z/P}(q) = q^{p-1}$$

ist. Wie in der vorstehenden Arbeit von Wegner folgt daraus nach der allgemeinen Diskriminantenformel für Z/P, daß $q = 2$ ist, und daß in der zugehörigen Verzweigungsgruppenreihe nur die erste Verzweigungsgruppe von 1 verschieden ist, die Ordnung 2^1 hat und mit der Vielfachheit 1 auftritt. Insbesondere ist daher die Verzweigungsordnung von 2 in Z/P von der Form

$$e = 2e_0 \quad \text{mit} \quad (e_0, 2) = 1.$$

Hieraus kann nach Artin (17) der Beitrag von 2 zum Führer

$$\mathfrak{f}_{Z/P} = \mathfrak{f}(\psi_1^0,\ Z/P)$$

berechnet werden, wo ψ_1^0 ein erzeugender Charakter der Galoisgruppe $\{T\}$ von Z/P ist. Es ergibt sich

$$\mathfrak{f}_{Z/P}(2) = 2^{\frac{1}{e}[(e-0)+(2-0)]} = 2^{1+\frac{2}{e}}.$$

Hiernach ist notwendig $e \mid 2$, also $e = 2$, und somit

$$\mathfrak{f}_{Z/P}(2) = 2^2.$$

Daß $e = 2$, also $e_0 = 1$ sein muß, ist ein Spezialfall der allgemeinen Tatsache, daß die Vielfachheiten v_i der Verzweigungsgruppen abelscher Körper sämtlich durch den primen Bestandteil e_0 der Verzweigungsordnung teilbar sind [5]; diese Tatsache folgt allgemein aus der Identität der formalen Artinschen Führer mit den klassenkörpertheoretisch definierten Führern im abelschen Falle, denn danach sind die Exponenten der Artinschen Führer ganzzahlig.

[5]) Siehe H. Hasse, Führer, Diskriminante und Verzweigungskörper relativ-abelscher Zahlkörper, Journ. f. Math. **162** (1930), 171.

Eingegangen 5. Mai 1936.

Über den Aufbau der Permutation geordneter Elemente.

Von *Franz Denk* in Erlangen.

§ 1. *Einleitung.*

1, 1. *Fragestellung.* Es soll sich im folgenden ausschließlich um Permutationen von Elementen handeln, die alle untereinander verschieden sind und welchen eine lineare Ordnung aufgeprägt ist, denen also z. B. die n ersten Zahlen der natürlichen Zahlenreihe zugeordnet sind. Letztere wollen wir deshalb als Elemente der hier betrachteten Permutationen ansehen. Zur Darstellung der Permutationen benutzen wir die *zweizeilige* Schreibweise:

$$P_n = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

oder die *einzeilige* Schreibweise:

$$P_n = (a_1 \quad a_2 \quad \dots \quad a_n).$$

Unter einem *oberen* bzw. *unteren* ν*-Intervall*, in Zeichen

$$J_{\mathrm{I}} = (x, x + \nu - 1) \quad \text{bzw.} \quad J_{\mathrm{II}} = (a_\mu, a_{\mu+\nu-1})$$

verstehen wir ν in der ersten bzw. in der zweiten Zeile der zweizeiligen Darstellung von P_n unmittelbar aufeinanderfolgende Elemente, deren erstes x bzw. a_μ sein soll. Besteht (für $1 < \nu < n$) ein Intervall J_{II} aus denselben[1]) Elementen wie ein Intervall J_{I}, so nennen wir ersteres eine (echte) Unterpermutation U_ν von P_n und schreiben einzeilig

$$U_\nu = (J_{\mathrm{II}})$$

oder zweizeilig

$$U_\nu = \begin{pmatrix} J_{\mathrm{I}} \\ J_{\mathrm{II}} \end{pmatrix} = \begin{pmatrix} x & x+1 & \dots & x+\nu-1 \\ a_\mu & a_{\mu+1} & \dots & a_{\mu+\nu-1} \end{pmatrix}.$$

Alle P_n, die keine Unterpermutationen enthalten, nennen wir *primitiv*, die übrigen *imprimitiv*.

Für $n \leqq 2$ können wir weder von primitiv noch von imprimitiv sprechen. Es ist zweckmäßig, die Permutationen

$$P_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{und} \quad P_2' \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

als *elementar* zu bezeichnen.

In den folgenden Zeilen sollen die primitiven und imprimitiven Permutationen etwas näher untersucht werden. Ich habe dabei eine Reihe von Bemerkungen und Ratschlägen, die ich Herrn Haupt verdanke, benützt.

[1]) Die Intervalle brauchen in den zwei Zeilen von P_n nicht unmittelbar untereinander zu stehen!

1, 2. *Geometrische Interpretation.* Es erweist sich als zweckmäßig, die Frage nach den primitiven und imprimitiven Permutationen in ein geometrisches Gewand zu kleiden.

Wir verbinden in der zweizeiligen Darstellung die Paare gleicher Zahlen (Elemente) durch Strecken. Die obere Zahl nennen wir *Anfangspunkt*, die untere *Endpunkt*, die Strecke selbst nennen wir *Sehne*, die Gesamtheit aller n Sehnen ein *Sehnengeflecht*.

Permutationen und Sehnengeflechte entsprechen einander eineindeutig.

Zu einer Unterpermutation (von v Elementen) gehören v Sehnen, von denen wir sagen, daß sie ein *Untergeflecht* bilden. Sehnengeflechte ohne Untergeflechte heißen primitiv, die übrigen imprimitiv.

Die gegenseitige Lage zweier Sehnen ist durch ihre Endpunkte a_r und a_s kennzeichenbar. Wir sagen: zwei Sehnen a_r und a_s *schneiden sich*, wenn ihre Endpunkte eine Inversion bilden [2]), wenn also $a_r > a_s$ mit $r < s$ ist.

Alle nicht zu einem Untergeflecht U gehörigen Sehnen eines Sehnengeflechtes P bilden wieder ein Sehnengeflecht C, aber im allgemeinen kein Untergeflecht von P. Wir bezeichnen C als *Komplement* von U in P, in Zeichen $C = P - U$.

Satz 1. *Eine beliebig vorgegebene Sehne des Komplementes $C = P - U$ wird entweder von allen oder von keiner Sehne des Untergeflechtes U geschnitten.*

Beweis. Es sei a_c eine *bestimmte* Sehne in C; dann ist entweder immer $c < u$ oder immer $c > u$ für *alle* Elemente a_u von U. Da ferner a_c nicht Element von U sein kann (Definition von C), so ist infolgedessen für *alle* a_u von U *entweder* $a_u < a_c$ *oder* $a_u > a_c$.

1, 3. *Klassenzerlegungen von $C = P - U$.* Wir können das Voranstehende auch etwas anders ausdrücken: Irgend zwei verschiedene Sehnen a_r und a_s wollen wir, soweit nur ihre gegenseitige Beziehung untersucht wird, ein *Paar* A nennen, in Zeichen $A = a_r \cdot a_s$. Je nachdem sich die Sehnen eines Paares *schneiden* oder *nicht schneiden*, bezeichnen wir das Paar als ein *Produkt* $a_r \times a_s$ oder als eine *Summe* $a_r \,||\, a_s$.

Irgend zwei (nicht notwendig elementfremde) Paare A_1 und A_2 bezeichnen wir als *positives* bzw. *negatives Doppelpaar* (A_1, A_2), je nachdem *beide* ein Produkt oder eine Summe bzw. das *eine* ein Produkt und das *andere* eine Summe darstellen.

Damit können wir aus unserem Satz folgern:

Ist a_n irgend eine Sehne eines Untergeflechtes U, so zerfallen die Sehnen des Komplementes $C = P - U$ in zwei Klassen; sind x und y Repräsentanten dieser zwei Klassen, und ist keine dieser Klassen leer, so ist $(x \cdot a_n, y \cdot a_n)$ negativ.

Ist eine dieser Klassen leer, so ist P reduzibel (vgl. **2**, 2).

1, 4. *Verschiedene Eigenschaften.* Für eine gegebene Permutation oder ein gegebenes Sehnengeflecht P definieren wir die folgenden Operationen:

I. Vertauscht man die beiden Zeilen einer Permutation miteinander, wird also das zugehörige Sehnengeflecht an einer wagerechten Achse gespiegelt, so nennen wir die neue Permutation die *reziproke Permutation P^{-1} von P*.

II. Stellen wir uns die Zeilen als feste Stangen $A——B$ und $A_1——B_1$ vor und drehen nun die untere Stange um eine Vertikalachse um 180° oder, schematisch dargestellt, bilden wir aus

$$A \,——\, B$$
$$A_1——B_1$$

[2]) Die Aufgabe, alle Permutationen von n Ziffern mit i Inversionen zu finden, behandelt O. Rodrigues, Journ. de Math. **4** (1839), p. 230—240.

die neue Permutation

$$A \text{ —— } B$$
$$B_1 \text{ —— } A_1,$$

so nennen wir diese die *umgedrehte Permutation zu P.*

III. Statt der unteren können wir jetzt auch die obere Stange um 180° drehen und erhalten so

$$B \text{ —— } A$$
$$A_1 \text{ —— } B_1.$$

Ersetzt man nun überall die Zahl i durch die Zahl $(n-1-i)$, so nennen wir die neue Permutation die *supplementäre Permutation zu P* [3]). Bedenken wir nun, daß bei diesen drei Operationen Untergeflechte wieder in Untergeflechte übergehen (und insbesondere leere Untergeflechte in leere Untergeflechte), daß ferner bei den Fällen I und III schneidende Paare in schneidende, nichtschneidende in nichtschneidende übergehen, während bei II schneidende und nichtschneidende Paare vertauscht werden, so ergibt sich:

Satz 2. *Primitivität bzw. Imprimitivität von P_n, ferner das Vorzeichen von Doppelpaaren sind gegenüber der Verwandlung von P_n in die dazu reziproke, umgedrehte oder supplementäre Permutation invariant.*

§ 2. *Über den Aufbau imprimitiver Permutationen.*

2, 1. *Definitionen.* Wir haben in Satz 1 (**1**, 2 und 3) gesehen, daß die Sehnen eines Untergeflechtes U von den Sehnen eines Teiles C' des Komplementes C geschnitten und von den Sehnen des anderen Teiles C'' nicht geschnitten werden. C kann (für imprimitive Sehnengeflechte) nicht leer sein, wohl aber seine Teile. Damit ergeben sich folgende zwei Möglichkeiten:

a) Wenigstens für *eine* Unterpermutation U von P ist C' oder C'' leer. Permutationen dieser Eigenschaft nennen wir *reduzibel.*

b) Für *alle* U von P ist keines der C' und C'' leer. Permutationen dieser Eigenschaft nennen wir *irreduzibel.*

2, 2. *Zerlegung der reduziblen Permutationen.* Wir untersuchen zuerst die reduziblen Sehnengeflechte eingehender. Setzen wir also z. B. $C'' = 0$ und $C' = V$. Seien $(2)_I$ und $(2)_{II}$ das obere bzw. untere Intervall von einem solchen U, für das $C'' = 0$ wird. Dann besteht der Rest der Zeile I aus zwei Teilintervallen $(1)_I$ und $(3)_I$, von denen wir annehmen können, daß sie vor bzw. hinter $(2)_I$ kommen. Nun müssen alle Sehnen, deren Anfangspunkte das Intervall $(1)_I$ bilden, die Sehnen von U schneiden, d. h. alle Endpunkte jener Sehnen (aber nur diese) bilden ein Intervall $(1)_{II}$, das hinter dem Intervall $(2)_{II}$ liegt. Umgekehrt liegt $(3)_I$ hinter $(2)_I$ und $(3)_{II}$ vor $(2)_{II}$. Dabei können (1) oder (3) auch leer sein oder aus einem einzigen Element bestehen.

Die beiden Intervalle $(1)_I$ $(2)_I$ und $(2)_{II}$ $(1)_{II}$ bestimmen zusammen jedenfalls eine Unterpermutation U_1, während $(3)_I$ und $(3)_{II}$ *entweder* eine dazu fremde Unterpermutation U_2 *oder* eine Einzelsehne E bestimmen. Damit ergibt sich:

Satz 3. *Jede reduzible Permutation läßt sich darstellen* a_1) *als Vereinigungsmenge zweier fremder Unterpermutationen, in Zeichen* $P = U_1 + U_2$, *oder* a_2) *als Vereinigungs-*

[3]) Vgl. Netto, Lehrbuch der Combinatorik, Leipzig 1927, § 66; dort werden in unseren Fällen II und III die Bezeichnungen *invers* bzw. *complementär* verwendet.

menge einer Unterpermutation und eines dazu fremden Elementes (einer dazu fremden Sehne), in Zeichen $P = U_1 + E$.

Betrachten wir also zuerst:

Fall a_1). $U_1 + U_2 = P$, Durchschnitt $U_1 \frown U_2$ leer, also $U_2 = P - U_1 = C_1$. Nach Satz 1 gibt es dann zwei Möglichkeiten: es werden entweder α) alle Sehnen von U_1 von allen Sehnen von U_2 geschnitten oder β) nicht geschnitten.

Im Falle α) sagen wir, U_1 *schneidet* U_2 $(= C_1)$ *in* P, und nennen U_1 und U_2 *Faktoren* von P; in Zeichen $P = U_1 \times U_2$. Im Falle β) sagen wir, U_1 *ist von* U_2 *(in* P*) abgetrennt*, und nennen U_1 und U_2 *Summanden* von P; in Zeichen $P = U_1 || U_2$. Beide Fälle gehen übrigens nach **1**, 4, II durch Bildung der entsprechenden umgedrehten Permutationen ineinander über.

Betrachten wir ferner:

Fall a_2). $U_1 + E = P$, $E =$ *Einzelsehne.*

Dann ist E nach **1**, 1 kein Untergeflecht, hat aber die Eigenschaft, daß sie alle übrigen Sehnen entweder schneidet oder nicht schneidet (da U_1 Untergeflecht aus $n - 1$ Sehnen ist). Auch in diesem Falle sprechen wir von Faktoren $(P = U_1 \times E)$ bzw. Summanden $(P = U_1 || E)$ und nennen E eine *Achse* (Schnittachse bzw. Trennachse).

2, 3. *Komponenten und Primkomponenten.* Um alle Fälle besser formulieren zu können, bezeichnen wir U_1 und C_1 (wobei auch $C_1 = E$ sein kann) in den beiden Fällen $P = U_1 \times C_1$ und $P = U_1 || C_1$ als die *Komponenten* K von P und schreiben für beide Fälle $P = K_1 \cdot K_2$. Beachten wir, daß K_1 und K_2 selbst wieder in Faktoren (oder Summanden) zerlegt werden können, und denken wir uns nun diese Zerlegung von Faktoren (nur) in Faktoren oder von Summanden (nur) in Summanden fortgesetzt, bis wir schließlich nicht weiter in Faktoren bzw. in Summanden zerlegen können, so bezeichnen wir diese alsdann auftretenden, nicht weiter zerlegbaren Komponenten als *Primfaktoren* π_ν bzw. als *Primsummanden* σ_ν (allgemein als *Primkomponenten*) von P; so ist also $P = \pi_1 \times \pi_2 \times \cdots$ bzw. $P = \sigma_1 || \sigma_2 || \cdots$. Bei dieser Zerlegung ist die Reihenfolge der Faktoren bzw. der Summanden naturgemäß nicht beliebig [4]).

Eine Zerlegung ergibt sich so: Da Fall a_1) oder a_2) vorliegt, kann angenommen werden, daß $K_1 \frown K_2$ leer ist und K_1 den Punkt 1, K_2 den Punkt n enthält. Es sei also z. B. $P = K_1 \times K_2$. Entweder ist dann K_1 Primfaktor und folglich K_2 ein Maximalfaktor, d. h. ein Faktor, der nicht (echtes) Untergeflecht eines größeren Faktors ist. Oder K_1 ist kein Primfaktor, kann also in (mindestens) zwei Faktoren K_1' und K_2'' zerlegt werden. Es möge dabei K_1' den Punkt 1 enthalten. Ist jetzt K_1' nicht Primfaktor, so kann es wieder zerlegt werden, usw.

Die Zerlegung ist *eindeutig*: Gehen wir nämlich von zwei Zerlegungen $P = K_1 \times K_2$ und $P = V_1 \times V_2$ aus, wobei jeweils der erste Faktor ein Primfaktor sein soll, dann ist entweder $K_1 = V_1$ oder z. B. $K_1 > V_1$; im letzteren Falle aber wäre V_1 Faktor von K_1, letzteres also kein Primfaktor, was der Voraussetzung widerspricht.

Alles übrige folgt durch vollständige Induktion.

Es ergibt sich damit:

Satz 4. (Zerlegungssatz für reduzible Permutationen). *Reduzible Permutationen lassen sich eindeutig zerlegen, entweder in lauter Primfaktoren* π, *die sich alle gegenseitig schneiden oder in lauter Primsummanden* σ, *die alle getrennt sind.*

2, 4. *Primkomponenten* 1., 2., 3. . . *Ordnung.* Primfaktoren können selbst wieder Summe von Primsummanden sein und umgekehrt. Wir unterscheiden daher: Prim-

[4]) Übrigens gehen beim Übergang von P in P^{-1} Faktoren in Summanden über und umgekehrt.

faktoren oder Primsummanden im Sinne von Satz 4, diese bezeichnen wir als *Primkomponenten erster Ordnung*; weiterhin Primkomponenten von Primkomponenten von P, die wir *Primkomponenten zweiter Ordnung* nennen. Entsprechend lassen sich Primkomponenten höherer Ordnung definieren.

Zufolge dieser Definition sind übrigens die Primkomponenten r-ter Ordnung dann Faktoren, wenn die Primkomponenten $(r-1)$-ter Ordnung Summanden sind und umgekehrt.

2, 5. *Bemerkung.* Sowohl an und für sich, als auch mit Hinblick auf gewisse Erweiterungsmöglichkeiten (allgemeine Untersuchung der Sehnenfiguren [5])) ist noch folgendes von Interesse:

Wir nennen ein Sehnengeflecht, dem man durch Einschalten von $2m$ neuen Anfangs- und Endpunkten *zwischen* je zwei der schon vorhandenen Anfangs- bzw. Endpunkte m, aber nicht mehr, (neue) Achsen hinzufügen kann, $(m+1)$-achsig [6]).

Nun gilt der

Satz 5. *Eine reduzible Permutation ist dann und nur dann k-achsig, wenn sie in k (und nicht mehr als k) Primkomponenten erster Ordnung zerlegbar ist.*

Irreduzible und primitive Permutationen sind einachsig.

Beweis. Es seien (1), (2), . . . die oberen und zugleich unteren Intervalle zu $\pi_1, \pi_2, \ldots$, dann ist für $P = \pi_1 \times \pi_2 \times \cdots$ symbolisch:

$$P = \begin{pmatrix} (1) & (2) & \ldots & (k+1) & (k) \\ (k) & (k+1) & \ldots & (2) & (1) \end{pmatrix}.$$

Zwischen zwei gleichbezeichnete Intervalle oben und unten läßt sich eine Achse einschalten, im ganzen also $(k-1)$ neue Achsen; P ist also k-achsig.

2, 6. *Irreduzible Permutationen.* Aus der Definition **2**, 1, b) erkennen wir, daß für irreduzible Permutationen niemals $U_1 + U_2 = P$ oder $U_1 + E = P$ (vgl. Satz 3) werden kann, weil man ja dann $U_2 = C_1'$, $C_2'' = 0$ (oder $E = C_1'$, $C_2'' = 0$) setzen könnte, was der Definition von **2**, 1, b) wiederspricht. Daraus folgt:

Satz 6. *Für irreduzible Permutationen gilt stets* $U_1 + U_2 < P$, $U_1 + E < P$, *wenn* U_1, U_2 *beliebige Unterpermutationen,* E *eine beliebige Einzelsehne von* P *bedeuten.*

Wir bezeichnen (allgemein) ein Untergeflecht als *maximal*, wenn es nicht *echter* Teil eines Untergeflechtes ist. Eine naheliegende Frage ist nun die nach dem Durchschnitt zweier maximaler Untergeflechte. Als *Durchschnitt* $U_1 \frown U_2$ bezeichnen wir dabei die Menge der Sehnen, welche beiden Untergeflechten gemeinsam sind. Für irreduzible Sehnengeflechte ist die Antwort einfach:

Satz 7. *In irreduziblen Permutationen sind maximale Unterpermutationen elementfremd* [7]).

Beweis (indirekt). Nehmen wir an, es gäbe zwei maximale Untergeflechte U_1 und U_2. Nach Voraussetzung ist dann aber $U_1 + U_2 < P$ jedenfalls kein Untergeflecht, denn sonst wäre z. B. U_1 nicht maximal. Haben nun U_1 und U_2 einen nicht leeren Durchschnitt, so müssen auch ihre beiden oberen bzw. unteren *Intervalle* einen nicht leeren

---

[5]) Über den Begriff vgl. Julius v. Sz. Nagy, Zur Topologie der geschlossenen Kurven auf der Sphäre, Acta litt. ac scient. Szeged **5** (1930—32), S. 1—12, insbes. S. 4—5.

[6]) Beachte: Um mehr-achsig zu sein, braucht ein Sehnengeflecht nicht selber Achsen zu enthalten.

[7]) In einer reduziblen Permutation sind maximale Untergeflechte nur dann elementfremd, wenn erstere zweiachsig ist (s. unten). Da diese Tatsache für uns hier nicht weiter von Bedeutung sein wird, so übergehen wir den (einfachen) Beweis.

Durchschnitt haben; d. h. $U_1 + U_2$ muß aus je einem oberen und einem unteren zusammenhängenden Intervall bestehen, bei dem die unteren Elemente eine Permutation der oberen sein müssen, $U_1 + U_2$ bildet also ein neues Untergeflecht, was dem eben Bewiesenen widerspricht.

Folgerung. Unser Satz gestattet uns, jedes irreduzible Sehnengeflecht zu zerlegen *in paarweise zueinander fremde maximale Untergeflechte und einen Rest, der kein Untergeflecht des ursprünglichen Sehnengeflechtes ist*, aber u. U. auch leer sein kann, und zwar ist die Zerlegung eindeutig bestimmt (Siehe auch **2, 7**) [8]).

2, 7. *Bestandteile höherer Ordnung.* Führen wir für maximale Untergeflechte von (wohlgemerkt nur) irreduziblen P_n wie für Primkomponenten von reduziblen P_n die gemeinsame Bezeichnung *Bestandteile von* P_n ein, so kann jeder Bestandteil wieder wie ein ursprüngliches Sehnengeflecht behandelt werden. Die Bestandteile von Bestandteilen bezeichnen wir dann als *Bestandteile zweiter Ordnung*, usw. Wir behaupten:

Die Bestandteile höchster (oder letzter) Ordnung in einem imprimitiven Sehnengeflecht sind entweder primitive oder elementare Untergeflechte (vgl. § 1). *Speziell können sie auch Einzelsehnen (nämlich Achsen der vorletzten oder der diesen vorausgehenden Bestandteile) sein.*

In der Tat: Ist ein Untergeflecht U weder primitiv noch elementar, so ist es imprimitiv, enthält also noch Untergeflechte. Letztere aber sind ganz oder teilweise enthalten entweder in einer Primkomponente von U (falls U selbst reduzibel ist) oder in einem maximalen Untergeflecht von U (falls dieses selbst irreduzibel ist).

Die Zerlegung in Bestandteile einzelner Ordnungen ist *eindeutig*; denn ein bestimmter Bestandteil (einer bestimmten Ordnung) ist *entweder* ein maximales Untergeflecht eines irreduziblen P_n *oder* eine Primkomponente eines reduziblen P_n, und daß die diesbezüglichen Zerlegungen in beiden Fällen eindeutig sind, haben wir bereits gesehen.

§ 3. *Über primitive Permutationen.*

3, 1. *Randsehnen.* Jedes der Elemente $1, n, a_1, a_n$ bezeichnen wir als Randelement oder *Randpunkt*, jede mindestens einen Randpunkt enthaltende Sehne als *Randsehne* von P_n. Jedes Sehnengeflecht hat *höchstens vier Randsehnen.*

Wir sehen jetzt alle zueinander supplementären, umgedrehten oder reziproken Permutationen und damit auch ihre Randsehnen als gleichwertig an.

Nur um uns auf ein bestimmtes Beispiel festzulegen, wollen wir im folgenden immer die durch die rechte Ecke (n) der ersten Zeile gehende Randsehne wählen.

Um nun den Aufbau der primitiven Permutationen zu klären, lassen wir das Element n fort; dann gibt es zwei Fälle:

Fall A). *Es bleibt eine primitive Permutation von* $n - 1$ *Elementen übrig.*

Fall B). *Es bleibt eine imprimitive Permutation* P_{n-1} *übrig.*

Zu Fall B) ist zu bemerken, daß die Sehne $(n - n)$ mindestens *eine*, aber nicht alle Sehnen eines Untergeflechtes von P_{n-1} schneiden muß. Denn sonst würde dieses Untergeflecht auch in P_{n-1} auftreten und P_n könnte nicht primitiv sein. Wegen der Primitivität von

---

[8]) Ersetzt man in diesem Falle alle maximalen Untergeflechte durch je eine einzige Sehne, so entsteht ein primitives Geflecht. — *Umgekehrt*: Ersetzt man in einem primitiven Sehnengeflecht jede Sehne durch ein Untergeflecht, so erhält man ein irreduzibles Sehnengeflecht, das uns aus maximalen Untergeflechten (ohne Rest) besteht. Während ein reduzibles Sehnengeflecht immer als Vereinigungsmenge zweier Untergeflechte (oder eines Untergeflechtes und einer Sehne) dargestellt werden kann, ist ein irreduzibles Sehnengeflecht (wenn überhaupt) nur als Vereinigungsmenge von mindestens vier paarweise fremden Untergeflechten darstellbar. —

P_n muß überdies die Hinzufügung der Sehne $(n - n)$ zu unserem P_{n-1} jedes Untergeflecht von P_{n-1} zerstören, d. h. n muß in das untere Intervall *eines jeden* Untergeflechtes von P_{n-1} fallen. Daher kann P_{n-1} nur ein *einziges* Untergeflecht (erster Ordnung) enthalten. Dieses fragliche Untergeflecht erster Ordnung kann aus dem gleichen Grunde nur ein Untergeflecht zweiter Ordnung enthalten, usw.

Damit bekommen wir als Ergebnis

Satz 8. *Läßt man aus einem primitiven Sehnengeflecht P_n eine Randsehne weg, so ist das übrigbleibende Geflecht P_{n-1} entweder* A) *selbst primitiv oder* B) *es enthält ein einziges (maximales) Untergeflecht erster Ordnung, das seinerseits wieder ein einziges (maximales) Untergeflecht zweiter Ordnung enthalten kann, usw.*

Im Falle A) ist die Strukturuntersuchung von primitiven P_n auf die von primitiven P_{n-1} zurückgeführt.

Im Falle B) aber haben wir die P_{n-1} auf ihre Irreduzibilität oder Reduzibilität hin zu untersuchen und weiter zu zerlegen. Die irreduziblen P_{n-1} sind durch Satz 8 genügend geklärt. Ist aber P_{n-1} reduzibel, so können höchstens zwei Primkomponenten auftreten, von denen eine eine Achse sein muß. Denn sonst enthielte P_{n-1} (im Widerspruch zu Satz 8) zwei (maximale) Untergeflechte. Weil P_{n-1} imprimitiv sein soll, müssen *genau* zwei Komponenten auftreten. Also:

Satz 9. *Läßt man aus einem primitiven Sehnengeflecht eine Randsehne weg und ist das übrigbleibende Geflecht reduzibel, so besteht es aus zwei Primkomponenten, von denen die eine eine Achse ist.*

3, 2. *Konstruktion.* Diese zwei Sätze gestatten uns, alle primitiven P_n zu konstruieren, wenn alle primitiven P_m $(m = 4, 5, \ldots, n - 1)$ bereits bekannt sind (für $n = 1, 2, 3$ gibt es keine primitiven P_n). Wir brauchen nur von *solchen* primitiven, irreduziblen und reduziblen P_{n-1} auszugehen, wie sie nach Satz 8 und 9 vorliegen müssen, und diesen P_{n-1} auf alle möglichen Arten eine n-te Sehne als Randsehne so hinzuzufügen, daß kein Untergeflecht entsteht bzw. ein vorhandenes Untergeflecht zerstört wird.

Die Durchführung dieses Verfahrens in den einzelnen Fällen bietet keinerlei Schwierigkeiten.

3, 3. *Schlußbemerkung.* Während die Untersuchung der imprimitiven Permutationen in gewissem Sinne als abgeschlossen angesehen werden kann, lassen sich bei den primitiven P weitere Strukturfragen stellen, auf die hier nicht eingegangen werden soll.

Eingegangen 28. April 1936.

Su due sistemi associati di infinite equazioni lineari.

Di *Ugo Broggi* a Milano.

Il problema della determinazione dei coefficienti γ_{rs} $(s = 1, 2, \ldots, r-1)$ del polinomio

$$(z+1)(z+2)\cdots(z+r-1) = z^{r-1} + \gamma_{r1}\, z^{r-2} + \cdots + \gamma_{r,r-1}$$

(le somme degli $\binom{r-1}{s}$ possibili prodotti di s fattori diversi scelti fra i numeri $1, 2, \ldots, r-1$), che prima di lui aveva occupato la Schläfli il Cayley il v. Zeipel lo Schlömilch, veniva ricondotto dal Nielsen a quello della formazione del polinomio $\psi_h(z)$, coefficiente della potenza $h+1$ di t nello sviluppo di

$$\left(\frac{1-e^{-t}}{t}\right)^{-z-1} = 1 + (1+z)\sum_{h=0}^{\infty} \psi_h(z)\, t^{h+1} \qquad (|t| < 2\pi).$$

É

$$\gamma_{rs} = \psi_{s-1}(r-1)\ ^{1}).$$

Ad una soluzione analoga perviene il Nörlund che sostituisce i polinomi di Nielsen con altri, che egli chiama polinomi di Bernoulli di ordine superiore, coi quali opera utilmente in altre ricerche. Ove si ponga col Nörlund

$$e^{zt}\left(\frac{t}{e^t-1}\right)^n = \sum_{\nu=0}^{\infty} \frac{t^\nu}{\nu!} B_\nu^{(n)}(z) \qquad (|t| < 2\pi)$$

e

$$B_\nu^{(n)}(0) = B_\nu^{(n)},$$

s'ottiene

$$\gamma_{rs} = (-1)^s \binom{r}{s} B_{r-s}^{(r+1)}\ ^{2}).$$

Il Nielsen determina i polinomi $\psi_h(z)$ il Nörlund i polinomi $B_\nu^{(n)}(z)$ per ricorrenza. Alla determinazione esplicita di γ_{rs} in funzione di r e di s si perviene invece, e direttamente, osservando che

$$\gamma_{r,r-1}\, z^{r-1} + \gamma_{r,r-2}\, z^{r-2} + \cdots + 1 = (r-1)!\left(\sum_{s=0}^{\infty} (-1)^s z^s\, \Delta^{r-1} O^{r+s-1}\right)^{-1}\ ^{3}).$$

---

[1]) Cfr. N. Nielsen, Recherches sur les polynômes et les nombres de Stirling, Annali di Matematica (3) **10** (1904), pp. 287—318.

[2]) Cfr. N. E. Nörlund, Vorlesungen über Differenzenrechnung, Berlin 1924, Kap. 6, § 5.

[3]) Cfr. U. Broggi, Sull' iterazione dell' operazione $x\frac{d}{dx}$, Rend. Lincei (6) **17** (1933), pp. 696—700.

Mi propongo di dimostrare qui che i numeri γ_{rs} $(s = 1, 2, \ldots, r-1)$ sono le $r-1$ incognite del sistema di $r-1$ equazioni lineari

$$h^{r-1} = \gamma_{r1} h^{r-2} - \gamma_{r2} h^{r-3} + \cdots + (-1)^{r-1} \gamma_{r,r-1} \qquad (h = 1, 2, \ldots, r-1)$$

che può assai agevolmente venire trasformato e risolto.

Si perviene al risultato ricordando che, come giá notava lo Stirling, se

$$\frac{A_0}{z} - \frac{A_1}{z^2} + \cdots \sim \frac{B_0}{z} - \frac{B_1}{z(z+1)} + \frac{B_2}{z(z+1)(z+2)} - \cdots$$

é anche

$$A_0 = B_0, \quad A_1 = B_1,$$

$$(1) \qquad B_r = A_r - \gamma_{r1} A_{r-1} + \gamma_{r2} A_{r-2} - \cdots + (-1)^{r-1} \gamma_{r,r-1} A_1 \quad [4])$$

e attraverso la considerazione dei due sistemi di infinite equazioni lineari con infinite incognite

$$\begin{aligned}
\text{I} \quad & \alpha'_0 + \alpha'_1 + \alpha'_2 + \cdots\cdots\cdots\cdots\cdots\cdots = A_0 \\
& 1^r \alpha'_1 + 2^r \alpha'_2 + \cdots\cdots\cdots\cdots\cdots\cdots = A_r \\
\text{II} \quad & \alpha''_0 + \alpha''_1 + \alpha''_2 + \cdots\cdots\cdots\cdots\cdots\cdots = B_0 \\
& r!\,\alpha''_r + \frac{(r+1)!}{1!}\alpha''_{r+1} + \frac{(r+2)!}{2!}\alpha'''_{r+2} + \cdots = B_r
\end{aligned}$$

$$(r = 1, 2, \ldots)$$

il primo dei quali é caso particolare dell'altro

$$\sum_{k=0}^{\infty} q_k^h x_h = A_k \qquad (h = 0, 1, \ldots),$$

dove q_k cresce indefinitamente con k, che E. Borel [5]) trattava nella sua tesi, mentre il secondo, ove l'integrale converga in corrispondenza di $r = 0, 1, \ldots$, ha la soluzione

$$\alpha_r = r! \int_0^{\infty} e^{-t} L_r(t) \left(\sum_{n=0}^{\infty} (-1)^n B_n \frac{t^n}{n!} \right) dt$$

dove

$$L_r(t) = \frac{e^t}{r!} \frac{d^r}{dt^r} (t^r e^{-t})$$

é il polinomio de Laguerre d'indice r [6]).

Mi propongo di dedurre della soluzione del secondo sistema una soluzione del primo, e d'indicare i limiti della validitá di questa.

I.

Ove l'ascissa di convergenza dell'integrale di Laplace

$$\int_0^1 t^{z-1} \varphi(t)\, dt$$

sia minore di $+\infty$ e sia legitima l'integrazione indefinita per parti, si ottiene se $Rz > 0$ e $\varphi(t)$ é limitata nell'intervallo chiuso $(0, 1)$

---

[4]) Cfr. ad es. N. Nielsen, Handbuch der Theorie der Gammafunktion, Leipzig 1906, §§ 26, 27, 109.

[5]) E. Borel, Sur quelques points de la théorie des fonctions, Annales de l'École Normale Sup. (3) **12** (1895), pp. 9—55, spec. pp . 38—44.

[6]) Cfr. U. Broggi, Su di un sistema di infinite equazioni lineari, Rend. Lincei (6) **22** (1935), pp. 120—124.

$$\int_0^1 t^{z-1}\,\varphi(t)\,dt = \left(\frac{1}{z}\,t^z\,\varphi(t)\right)_0^1 - \frac{1}{z}\int_0^1 t^z\,\varphi'(t)\,dt = \cdots$$

$$\sim \frac{\varphi(1)}{z} - \frac{\varphi'(1)}{z(z+1)} + \frac{\varphi''(1)}{z(z+1)(z+2)} - \cdots;$$

$$\int_0^1 t^{z-1}\,\varphi(t)\,dt = \left(\frac{1}{z}\,t^z\,\varphi(t)\right)_0^1 - \frac{1}{z}\int_0^1 t^{z-1}\,(t\varphi'(t))\,dt$$

$$= \frac{\varphi(1)}{z} - \frac{\varphi_1(1)}{z^2} + \frac{1}{z^2}\int_0^1 t^{z-1}\,(t\varphi_1'(t))\,dt$$

$$= \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\sim \frac{\varphi(1)}{z} - \frac{\varphi_1(1)}{z^2} + \frac{\varphi_2(1)}{z^3} - \cdots,$$

dove

$$\varphi_0(t) = \varphi(t), \qquad \varphi_n(t) = t\,\varphi_{n-1}'(t) \qquad (n = 1, 2, \ldots).$$

Se in particolare lo sviluppo

$$\varphi(t) = \alpha_0 + \alpha_1\,t + \cdots$$

ha un raggio di convergenza maggiore di 1, ed é

$$\varphi^{(n)}(1) = B_n$$

si ha evidentemente

$$\alpha_0 + \alpha_1 + \alpha_2 + \cdots\cdots\cdots\cdots\cdots = B_0$$

$$r!\,\alpha_r + \frac{(r+1)!}{1!}\,\alpha_{r+1} + \frac{(r+2)!}{2!}\,\alpha_{r+2} + \cdots = B_r$$

cosí come si ha

$$\alpha_0 + \alpha_1 + \alpha_2 + \cdots = A_0$$

$$1^r\,\alpha_1 + 2^r\,\alpha_2 + \cdots = A_r$$

$$(r = 1, 2, \ldots)$$

se

$$A_r = \varphi_r(1).$$

E poiché é anche

$$B_r = \sum_{n=r}^{\infty} n(n-1)\cdots(n-r+1)\,\alpha_n$$

$$= \sum_{n=r}^{\infty} n^r\,\alpha_n - \left(\sum_{n=r}^{\infty} n^{r-1}\,\alpha_n\right)\gamma_{r1} + \cdots + (-1)^{r-1}\,\gamma_{r,r-1}\left(\sum_{n=r}^{\infty} n\,\alpha_n\right)$$

$$= \left[A_r - \sum_{s=1}^{r-1} s^r\,\alpha_s\right] - \gamma_{r1}\left[A_{r-1} - \sum_{s=1}^{r-1} s^{r-1}\,\alpha_s\right] + \cdots + (-1)^{r-1}\,\gamma_{r,r-1}\left[A_1 - \sum_{s=1}^{r-1} s\alpha_s\right],$$

se ne deduce, per la (1)

$$B_r = A_r - \gamma_{r1}\,A_{r-1} + \cdots + (-1)^{r-1}\,A_1 \qquad (1)$$

che

$$h^{r-1} = \gamma_{r1}\,h^{r-2} - \gamma_{r2}\,h^{r-3} + \cdots + (-1)^r\,\gamma_{r,r-1}$$

$$(h = 1, 2, \ldots, r-1).$$

Il sistema di $r-1$ equazioni lineari con $r-1$ incognite $\gamma_{r1}, \gamma_{r2}, \ldots, \gamma_{r,r-1}$ così ottenuto

$$\begin{aligned}
1^{r-1} &= \gamma_{r1} - \gamma_{r2} + \gamma_{r3} - \cdots + (-1)^{r-2}\gamma_{r,r-1} \\
2^{r-1} &= 2^{r-2}\gamma_{r1} - 2^{r-3}\gamma_{r2} + \cdots + (-1)^{r-2}\gamma_{r,r-1} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
(r-1)^{r-1} &= (r-1)^{r-2}\gamma_{r1} - (r-1)^{r-3}\gamma_{r2} + \cdots + (-1)^{r-2}\gamma_{r,r-1}
\end{aligned}$$

si trasforma immediatamente nell'altro

$$\begin{aligned}
\Delta^{r-2}1^{r-1} &= (r-2)!\,\gamma_{r1} \\
\Delta^{r-3}1^{r-1} &= \gamma_{r1}\Delta^{r-3}1^{r-2} - (r-3)!\,\gamma_{r2} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\Delta^{r-s-1}1^{r-1} &= \gamma_{r1}\Delta^{r-s-1}1^{r-2} - \gamma_{r2}\Delta^{r-s-1}1^{r-3} + \cdots + (-1)^{s-1}(r-s-1)!\,\gamma_{rs} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
1^{r-1} &= \gamma_{r1} - \gamma_{r2} + \cdots + (-1)^{r-1}\gamma_{r,r-1}
\end{aligned}$$

che fornisce

$$\gamma_{r1} = \frac{1}{(r-2)!}\Delta^{r-2}1^{r-1}$$

$$\gamma_{r2} = \frac{1}{(r-2)!\,(r-3)!}\begin{vmatrix} \Delta^{r-2}1^{r-1} & \Delta^{r-3}1^{r-1} \\ \Delta^{r-2}1^{r-2} & \Delta^{r-3}1^{r-2} \end{vmatrix}.$$

Si ha cioé, se $s = 1, 2$

$$\gamma_{rs} = \frac{1}{(r-2)!\,(r-3)!\cdots(r-s-1)!}\begin{vmatrix} \Delta^{r-2}1^{r-1} & \Delta^{r-3}1^{r-1} & \cdots & \Delta^{r-s-1}1^{r-1} \\ \Delta^{r-2}1^{r-2} & \Delta^{r-3}1^{r-2} & \cdots & \Delta^{r-s-1}1^{r-2} \\ 0 & \Delta^{r-3}1^{r-3} & \cdots & \Delta^{r-s-1}1^{r-3} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \Delta^{r-s-1}1^{r-s} \end{vmatrix}$$

: che l'espressione ottenuta sussista qualunque sia s se essa vale in corrispondenza di $s-1, s-2, \ldots, 2, 1$, lo si vede sviluppando il determinante del secondo membro secondo gli elementi della sua ultima colonna. Si ottiene infatti

$$\frac{1}{(r-2)!\,(r-3)!\cdots(r-s)!}\begin{vmatrix} \Delta^{r-2}1^{r-1} & \Delta^{r-3}1^{r-1} & \cdots & \Delta^{r-s-1}1^{r-1} \\ \Delta^{r-2}1^{r-2} & \Delta^{r-3}1^{r-2} & & \Delta^{r-s-1}1^{r-2} \\ 0 & \Delta^{r-3}1^{r-3} & & \Delta^{r-s-1}1^{r-3} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & & \Delta^{r-s-1}1^{r-s} \end{vmatrix}$$

$$= (-1)^{s-1}\left\{\Delta^{r-s-1}1^{r-1} - \Delta^{r-s-1}1^{r-2}\frac{\Delta^{r-2}1^{r-1}}{(r-2)!} + \Delta^{r-s-1}1^{r-3}\frac{1}{(r-2)!\,(r-3)!}\begin{vmatrix} \Delta^{r-2}1^{r-1} & \Delta^{r-3}1^{r-1} \\ \Delta^{r-2}1^{r-2} & \Delta^{r-3}1^{r-2} \end{vmatrix} - \cdots\right.$$

$$= (-1)^{s-1}\left\{\Delta^{r-s-1}1^{r-1} - \gamma_{r1}\Delta^{r-s-1}1^{r-2} + \gamma_{r2}\Delta^{r-s-1}1^{r-3} - \cdots + (-1)^{s-1}\gamma_{r,s-1}\Delta^{r-s-1}1^{r-s-1}\right\}$$

$$= (-1)^{s-1}(r-s-1)!\,\gamma_{rs}$$

come risulta dalla s-esima equazione del sistema trasformato.

Se ne ha in particolare, se $s = r-1$, poiché $\gamma_{r,r-1} = (r-1)!$

$$1!\,2!\cdots r! = \begin{vmatrix} 1 & 1^2 & \cdots & 1^r \\ \Delta 1 & \Delta 1^2 & \cdots & \Delta 1^r \\ 0 & \Delta^2 1^2 & \cdots & \Delta^2 1^r \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \Delta^{r-1}1^r \end{vmatrix}.$$

II.

Se il punto $z = 1$ è interno al poligono di Borel della serie $\sum_{n=0}^{\infty} (-1)^n B_n z^n$

$$\alpha_r = r! \int_0^{\infty} e^{-t} L_r(t) \left(\sum_{n=0}^{\infty} (-1)^n B_n \frac{t^n}{n!} \right) dt \qquad (r = 0, 1, \ldots),$$

é la somma generalizzata di Borel della serie

$$\sum_{n=0}^{\infty} (-1)^n n(n-1) \cdots (n-r+1) B_n$$

: il sistema di infinite equazioni lineari con infinite incognite

$$\text{II} \quad \begin{aligned} &\alpha_0'' + \alpha_1'' + \alpha_2'' + \cdots\cdots\cdots\cdots\cdots\cdots = B_0 \\ &r!\,\alpha_r'' + \frac{(r+1)!}{1!}\alpha_{r+1}'' + \frac{(r+2)!}{2!}\alpha_{r+2}'' + \cdots = B_r \end{aligned}$$

ha la soluzione

$$\alpha_r'' = r! \int_0^{\infty} e^{-t} L_r(t) \left(\sum_{n=0}^{\infty} (-1)^n B_n \frac{t^n}{n!} \right) dt \ [7]).$$

Ci proponiamo di dedurre da essa una soluzione del sistema

$$\text{I} \quad \begin{aligned} &\alpha_0' + \alpha_1' + \alpha_2' + \cdots = A_0 \\ &1^r \alpha_1' + 2^r \alpha_2' + \cdots = A_r \\ &(r = 1, 2, \ldots) \end{aligned}$$

e di determinare le condizioni alle quali debbono soddisfare gli elementi della successione $A_0, A_1, \ldots$ perché questa soluzione sia valida.

Perveniamo allo scopo ricordando che, come veniva dimostrato dal Nörlund, se la funzione

$$f(t) = A_0 + A_1 \frac{t}{1!} + \cdots$$

é olomorfa in un angolo che comprende il semiesse reale e positivo e si ha uniformemente in questo angolo

$$\lim_{t \to \infty} e^{-\varkappa t} f^{(p)}(t) = 0 \qquad (p = 0, 1, \ldots;\ \varkappa > 0)$$

la serie

$$\frac{A_0}{z} - \frac{A_1}{z^2} + \cdots,$$

che puó divergere in corrispondenza di ogni valore di z, é assolutamente ed uniformemente sommabile secondo Borel e la sua somma

$$F(z) = \frac{1}{z} \int_0^{\infty} e^{-tz} f\left(\frac{t}{z}\right) dt$$

coincide se z é reale e positivo, con

$$\Phi(z) = \int_0^{\infty} e^{-tz} f(t)\, dt. \qquad (2)$$

Le due funzioni uniformi $F(z)$, $\Phi(z)$ coincidenti nei punti del semiasse reale e positivo interni al semipiano di convergenza dell'integrale di Laplace (2), sono espressioni

---

[7]) Cfr. U. Broggi, loc. cit. [6]).

diverse di una stessa funzione

$$F(z) = \int_0^\infty e^{-tz} f(t)\, dt$$

suscettibile di uno sviluppo in serie di fattoriali

$$\sum_{s=0}^{\infty} \frac{c_s \omega^s}{z(z+\omega)\cdots(z+s\omega)}$$

: perché, come a noi importa, possa attribuirsi ad ω il valore 1, la funzione

$$\varphi(t) = f(-\log t) = \sum_0^\infty (-1)^n B_n (1-t)^n$$

deve essere olomorfa nel circolo $|t-1| = 1$. Deve essere pertanto

$$\limsup \sqrt[n]{|B_n|} \leqq 1 \quad [8]). \tag{3}$$

L'integrale

$$\int_0^\infty e^{-t} L_r(t) \left(\sum_{n=0}^{\infty} (-1)^n B_n \frac{t^n}{n!} \right) dt$$

converge qualunque sia r e definisce $\frac{1}{r!}\alpha'_r$ $(r = 0, 1, \ldots)$, se il primo membro della (3) é minore del secondo, o se, essendo uguale, il punto $t=1$ é punto regolare di $B_0 - B_1 t + \cdots$ e pertanto interno al poligono di Borel corrispondente alla serie.

[8]) Cfr. N. E. Nörlund, Leçons sur les séries d'interpolation, Paris 1926, pp. 184—188.

Eingegangen 29. April 1936.

Theorie der quadratischen Formen in beliebigen Körpern.

Von *Ernst Witt* in Göttingen.

Die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Koeffizienten rational ineinander transformiert werden können, sind zuerst von *Minkowski* (**5**) aufgestellt worden [1]). Aufbauend auf seine Theorie der ganzzahligen quadratischen Formen zeigte er, daß sich aus einer Form f für jede Primzahl p in gewisser Weise eine *Einheit* $C_p(f) = \pm 1$ herstellen läßt, die bei allen Transformationen der Form ungeändert bleibt; und er sprach den Satz aus, daß zwei Formen mit gleicher Diskriminante, gleichem Sylvesterschen Trägheitsindex und gleichen Einheiten C_p immer rational ineinander transformiert werden können. Er löste auch die Frage, unter welchen Umständen eine Form die Null rational darstellen kann, und er gab an, bei welchen Zusammenstellungen der Invarianten es zugehörige quadratische Formen wirklich gibt.

In einer Reihe von Arbeiten hat dann *Hasse* (**3**) die Sätze von Minkowski mit einer übersichtlichen, von Hensel eingeführten Behandlungsweise (*Schluß vom Kleinen aufs Große*) hergeleitet; er hat diese Sätze auch für ganz beliebige Zahlkörper verallgemeinert. Die Minkowskischen Einheiten C_p konnten durch *Hilbertsche Normrestsymbole* $\left(\frac{a, b}{p}\right)$ ersetzt werden, dadurch wurden die Beweise unabhängig von der weitläufigen Theorie der ganzzahligen Formen.

Da aus der neueren Theorie der Algebren bekannt ist, daß eine Algebra (a, b) im wesentlichen dasselbe ist wie ein System von Normrestsymbolen, hat *Artin* in einer Vorlesung die quadratischen Formen von vornherein auf dieser Grundlage behandelt. Er ordnete jeder *Form*

$$f = \sum_1^n a_i x_i^2$$

die *Algebra*

$$S(f) = \prod_{i \leq k} (a_i, a_k)$$

zu. Die Invarianz dieser Algebra bei allen Transformationen war allerdings nicht ganz leicht einzusehen, und so erhob sich die Forderung, ein anderes hyperkomplexes System ausfindig zu machen, für welches die Invarianz direkt ersichtlich ist, und aus welchem sich die Algebra $S(f)$ in einfacher Weise gewinnen läßt. Dies geschieht in dieser Arbeit durch Angabe des **Systems** $C(f)$ *vom Rang* 2^n *mit den Erzeugenden* $u_1, \ldots, u_n$ *und den definierenden Relationen* $u_i^2 = a_i$, $u_i u_k = -u_k u_i$ $(i \neq k)$. Historisch ist zu bemerken, daß diese hyperkomplexen Zahlen für den Fall $a_i = -1$ bereits von *Clifford* (**2**) als Verallgemeinerung der Quaternionen betrachtet wurden.

[1]) Die eingeklammerten Zahlen in Fettdruck verweisen auf die entsprechende Arbeit im Literaturverzeichnis auf S. 44.

In ganz beliebigen Körpern (der Charakteristik $\neq 2$) liefert die Algebra $S(f)$ zusammen mit der Diskriminante für $n = 1, 2, 3$ ein volles Invariantensystem bezüglich der Äquivalenz der quadratischen Formen, und für $n = 1, 2, 3, 4$ lassen sich allgemeingültige Bedingungen dafür angeben, wann eine Form die Null darstellt (vgl. die Tabelle auf S. 39). Nach einer einfachen Bemerkung von Hensel (**4**) folgen daraus sofort Kriterien dafür, wann irgendeine Zahl $m \neq 0$ von einer Form dargestellt wird (für $n = 1, 2, 3$).

Im Anfang der Arbeit werden bei beliebigen Körpern allgemeine Theoreme über quadratische Formen hergeleitet, die zwar mit den einfachsten Mitteln beweisbar sind, dennoch bisher wohl unbekannt waren, wie z. B. der Satz, daß aus der Äquivalenz von $f + g$ mit $f + h$ die andere Äquivalenz von g mit h folgt. In dieser Theorie spielen diejenigen Formen, welche die Null nicht darstellen, eine wichtige Rolle. Bei geeigneter Komposition bilden sie die Elemente eines **Ringes** (ebenso, wie in der Algebrentheorie die Schiefkörper Elemente einer Gruppe sind).

Indem wir uns auf diese allgemeinen Sätze stützen, können wir in vielen Körpern, in denen die Algebrentheorie schon erforscht ist, alle diejenigen Fragen lösen, welche von Minkowski und Hasse für den Fall eines Zahlkörpers untersucht worden sind. Die Hauptsätze über quadratische Formen mit Koeffizienten aus einem Zahlkörper werden hier noch einmal kurz als Anwendung der allgemeinen Theorie dargestellt (vgl. die Tabelle auf S. 42). Für viele interessante Spezialfälle der Hauptsätze, die hier nicht aufgenommen sind, verweisen wir auf die Arbeiten von Hasse (**3**).

Als letztes Beispiel werden quadratische Formen in einem reellen Funktionenkörper vollständig behandelt. Hier wird z. B. die Äquivalenz durch unendlich viele Trägheitsindizes geregelt.

I. Metrische Räume.

Einführung. Es sei ein fester Koeffizientenkörper K zugrundegelegt, die Charakteristik sei $\neq 2$.

Mit Hilfe einer quadratischen Form (Metrik)

$$f = \sum_{i,k} a_{ik} x_i x_k \qquad (a_{ik} = a_{ki};\ i, k = 1, \ldots, n)$$

machen wir den n-dimensionalen Vektorraum

$$\mathfrak{R} = \langle K\mathfrak{u}_1, \ldots, K\mathfrak{u}_n \rangle$$

zu einem metrischen Raum, indem wir in ihm ein (inneres) Produkt zweier Vektoren erklären durch

$$\sum_i x_i \mathfrak{u}_i \cdot \sum_k y_k \mathfrak{u}_k = \sum_{i,k} a_{ik} x_i y_k .$$

Eine Basisänderung entspricht dem Übergang zu einer äquivalenten quadratischen Form. Die Diskriminante $|\mathfrak{u}_i \mathfrak{u}_k| = |a_{ik}|$ multipliziert sich dabei stets mit einer Quadratzahl $\neq 0$ aus dem Körper K. Diese bis auf Quadratzahlen festgelegte Zahl $|\mathfrak{u}_i \mathfrak{u}_k|$ bezeichnen wir mit $|\mathfrak{R}|$ oder mit $d(f)$.

Besteht zwischen zwei Räumen eine additions- und multiplikationstreue Zuordnung, so sollen sie isomorph heißen. Äquivalente Formen $f_1 \cong f_2$ bestimmen also isomorphe Räume $\mathfrak{R}_1 \cong \mathfrak{R}_2$, und umgekehrt. Eindimensionale Räume sind schon durch die Diskriminante $|\mathfrak{R}|$ bis auf Isomorphie festgelegt.

Wenn $\mathfrak{u}\mathfrak{v} = 0$ ist, sagen wir, die Vektoren $\mathfrak{u}$ und $\mathfrak{v}$ stehen senkrecht aufeinander. Mit $\mathfrak{R} = \mathfrak{R}_1 + \mathfrak{R}_2$ bezeichnen wir die Zerlegung in senkrechte Teilräume.

Untersuchung. Diejenigen Vektoren $\sum_i x_i \mathfrak{u}_i$, welche auf *allen* Vektoren von $\mathfrak{R}$ senkrecht stehen, bilden einen Teilraum $\mathfrak{R}_0$, das **Radikal** von $\mathfrak{R}$. Da sich der Wert eines

Vektorproduktes nicht ändert, wenn die Faktoren mod. $\mathfrak{R}_0$ abgeändert werden, ist es sinnvoll, von einem Raume $\mathfrak{R}/\mathfrak{R}_0$ zu reden. Wegen

$$\mathfrak{R} \cong \mathfrak{R}_0 + \mathfrak{R}/\mathfrak{R}_0$$

hängt die Beschaffenheit des Raumes $\mathfrak{R}$ nur von der Struktur des durch $\mathfrak{R}$ eindeutig bestimmten Raumes $\mathfrak{R}/\mathfrak{R}_0$ ab; dieser Raum $\mathfrak{R}/\mathfrak{R}_0$ hat kein Radikal mehr.

Es genügt daher, *von jetzt ab einen Raum $\mathfrak{R}$ ohne Radikal* zu untersuchen. Das Fehlen des Radikals ist gleichbedeutend mit der Unlösbarkeit des Gleichungssystems $\sum_i x_i u_i u_k = 0$ $(k = 1, \ldots, n)$, d. h. *die Diskriminante $|\mathfrak{R}|$ darf nicht verschwinden.*

Die Grundlage zu einer übersichtlichen Strukturuntersuchung der metrischen Räume ohne Radikal liefert

Satz 1. *$\mathfrak{r}$ sei ein Teilraum von $\mathfrak{R}$, und $\mathfrak{r}^*$ sei der zu $\mathfrak{r}$ senkrechte Teilraum. Dann gilt*

$$\dim \mathfrak{r} + \dim \mathfrak{r}^* = \dim \mathfrak{R}, \tag{1}$$

$$\mathfrak{r}^{**} = \mathfrak{r}. \tag{2}$$

Wenn $|\mathfrak{r}| \neq 0$ ist, so ist auch $|\mathfrak{r}^*| \neq 0$, und es gilt

$$\mathfrak{R} = \mathfrak{r} + \mathfrak{r}^*, \tag{3}$$

$$|\mathfrak{R}| = |\mathfrak{r}| \cdot |\mathfrak{r}^*|. \tag{4}$$

Beweis. Wir dürfen $\mathfrak{r} = \langle u_1, \ldots, u_r \rangle$ annehmen. $\mathfrak{r}^*$ besteht aus allen Vektoren $\sum_i x_i u_i$ mit $\sum_i x_i u_i u_k = 0$ $(k = 1, \ldots, r)$. Wegen $|\mathfrak{R}| \neq 0$ hat dieses Gleichungssystem den Rang r und damit $n - r$ linear unabhängige Lösungen. — Aus (1) folgt $\dim \mathfrak{r}^{**} = \dim \mathfrak{r}$, andererseits ist logisch klar, daß $\mathfrak{r}^{**} \supseteq \mathfrak{r}$ gilt; damit ist (2) bewiesen. — Wenn $\mathfrak{r}$ kein Radikal hat, gilt $\mathfrak{r} \cap \mathfrak{r}^* = 0$. Wegen (1) folgt jetzt (3). Wir dürfen $\mathfrak{r}^* = \langle u_{r+1}, \ldots, u_n \rangle$ annehmen, daraus ist die Gültigkeit von (4) ersichtlich, und aus (4) folgt $|\mathfrak{r}^*| \neq 0$.

Die bekannte Tatsache, daß es zu jeder quadratischen Form eine äquivalente Diagonalform gibt, in der eine beliebige durch die Form darstellbare Zahl $a \neq 0$ als erster Koeffizient erscheint, ist eine unmittelbare Folge von Satz 1. Wir sprechen sie nur in einer anderen, aber gleichwertigen Form aus:

Satz 2. *Ist $\mathfrak{v}_1$ ein beliebiger Vektor, dessen Quadrat nicht verschwindet, so gibt es eine orthogonale Zerlegung*

$$\mathfrak{R} = \langle \mathfrak{v}_1 \rangle + \cdots + \langle \mathfrak{v}_n \rangle.$$

Beweis durch Induktion. Wegen $|\mathfrak{R}| \neq 0$ verschwinden nicht alle Vektorprodukte, und wegen $4\mathfrak{u}\mathfrak{v} = (\mathfrak{u} + \mathfrak{v})^2 - (\mathfrak{u} - \mathfrak{v})^2$ auch nicht alle Vektorquadrate (Charakteristik $\neq 2$!). Es sei $\mathfrak{v}_1^2 \neq 0$. Nach Satz 1 folgt eine Zerlegung $\mathfrak{R} = \langle \mathfrak{v}_1 \rangle + \langle \mathfrak{v}_1 \rangle^*$. Für den Teilraum $\langle \mathfrak{v}_1 \rangle^*$ dürfen wir aber schon eine Zerlegung $\langle \mathfrak{v}_1 \rangle^* = \langle \mathfrak{v}_2 \rangle + \cdots + \langle \mathfrak{v}_n \rangle$ ansetzen.

In besonderen Fällen läßt sich zu einer quadratischen Form eine zugehörige Diagonalform explizit angeben:

Satz 3. *Sind alle Teildeterminanten*

$$d_r = \begin{vmatrix} a_{11} & \cdots & a_{1r} \\ \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{rr} \end{vmatrix} \neq 0 \quad \textit{für} \quad r = 1, \ldots, n,$$

so ist

$$\sum_{i,k} a_{ik} x_i x_k \cong \sum_i \frac{d_i}{d_{i-1}} y_i^2 \qquad (d_0 = 1).$$

Beweis durch Induktion. Für den Teilraum $\mathfrak{r} = \langle \mathfrak{u}_1, \ldots, \mathfrak{u}_{n-1} \rangle$ dürfen wir eine Zerlegung $\mathfrak{r} = \langle \mathfrak{v}_1 \rangle + \cdots + \langle \mathfrak{v}_{n-1} \rangle$ ansetzen mit $\mathfrak{v}_i^2 = \frac{d_i}{d_{i-1}}$. Nach Satz 1 ist $\mathfrak{R} = \mathfrak{r} + \langle \mathfrak{v}_n \rangle$ und $\mathfrak{v}_n^2 \cong \frac{d_n}{d_{n-1}}$. (Dabei bedeute $a \cong b$, daß $\frac{a}{b}$ eine Quadratzahl ist.)

Für die weitere Entwicklung brauchen wir einen

Hilfssatz. *Alle binären Formen $ax^2 + 2bxy + cy^2$, welche die Null (in nicht trivialer Weise) darstellen, sind untereinander äquivalent.*

Beweis. Die Nulldarstellung bedeutet: Es gibt in $\mathfrak{R}$ einen Vektor $\mathfrak{u} \neq 0$ mit $\mathfrak{u}^2 = 0$. Wegen $|\mathfrak{R}| \neq 0$ gibt es einen Vektor $\mathfrak{w}$ mit $\mathfrak{u}\mathfrak{w} = 1$. Es sei $\mathfrak{v} = 2\mathfrak{w} - \mathfrak{w}^2\mathfrak{u}$. Für $\mathfrak{u}, \mathfrak{v}$ lautet die Produkttafel $\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$. Folglich ist die gegebene Form mit der festen Form $4xy$ äquivalent. — Eine andere Normalform ist z. B. $x^2 - y^2$.

Nun sind wir in der Lage, einen wichtigen Kürzungssatz zu beweisen.

Satz 4. *Aus $\mathfrak{R}_1 + \mathfrak{R}_3 \cong \mathfrak{R}_2 + \mathfrak{R}_3$ darf $\mathfrak{R}_1 \cong \mathfrak{R}_2$ geschlossen werden.*

Beweis. Da $\mathfrak{R}_3$ entsprechend Satz 2 zerlegt werden kann, genügt es, $\mathfrak{R}_3$ als eindimensional anzunehmen. Setzen wir $\mathfrak{R} = \mathfrak{R}_1 + \mathfrak{R}_3$, so können wir die Behauptung auch folgendermaßen formulieren: Aus $\mathfrak{u}^2 = \mathfrak{v}^2 \neq 0$ folgt $\langle \mathfrak{u} \rangle^* \cong \langle \mathfrak{v} \rangle^*$.

Wenn $\langle \mathfrak{u}, \mathfrak{v} \rangle$ eindimensional ist, so ist sogar $\langle \mathfrak{u} \rangle^* = \langle \mathfrak{v} \rangle^*$. Es sei jetzt $\langle \mathfrak{u}, \mathfrak{v} \rangle$ zweidimensional.

Wenn die Diskriminante $|\mathfrak{u}, \mathfrak{v}| \neq 0$ ist, so gilt nach Satz 1

$$\mathfrak{R} = \langle \mathfrak{u}, \mathfrak{v} \rangle + \langle \mathfrak{u}, \mathfrak{v} \rangle^* \quad \text{und} \quad \langle \mathfrak{u}, \mathfrak{v} \rangle = \langle \mathfrak{u} \rangle + \mathfrak{U} = \langle \mathfrak{v} \rangle + \mathfrak{V};$$

dabei müssen $\mathfrak{U}$ und $\mathfrak{V}$ als eindimensionale Räume mit gleicher Diskriminante äquivalent sein. Also ist

$$\langle \mathfrak{u} \rangle^* = \mathfrak{U} + \langle \mathfrak{u}, \mathfrak{v} \rangle^* \cong \mathfrak{V} + \langle \mathfrak{u}, \mathfrak{v} \rangle^* = \langle \mathfrak{v} \rangle^*.$$

Ist endlich $|\mathfrak{u}, \mathfrak{v}| = 0$, so läßt sich eine neue Basis $\mathfrak{u}_0, \mathfrak{u}_1$ mit der Produkttafel $\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$ angeben ($a \neq 0$). Da $\mathfrak{R}$ kein Radikal besitzt, gibt es einen Vektor $\mathfrak{u}_2$ mit $\mathfrak{u}_0\mathfrak{u}_2 = 1$. Für $\mathfrak{u}_0, \mathfrak{u}_1, \mathfrak{u}_2$ lautet die Produkttafel $\begin{pmatrix} 0 & 0 & 1 \\ 0 & a & * \\ 1 & * & * \end{pmatrix}$, diese Vektoren spannen also einen dreidimensionalen Raum $\mathfrak{r}$ mit $|\mathfrak{r}| \neq 0$ auf. Es gilt

$$\mathfrak{R} = \mathfrak{r} + \mathfrak{r}^* \quad \text{und} \quad \mathfrak{r} = \langle \mathfrak{u} \rangle + \mathfrak{U} = \langle \mathfrak{v} \rangle + \mathfrak{V}.$$

Dabei enthalten $\mathfrak{U}$ und $\mathfrak{V}$ beide den Vektor $\mathfrak{u}_0$ mit $\mathfrak{u}_0^2 = 0$, sind also nach dem Hilfssatz isomorphe Räume. Nun folgt

$$\langle \mathfrak{u} \rangle^* = \mathfrak{U} + \mathfrak{r}^* \cong \mathfrak{V} + \mathfrak{r}^* = \langle \mathfrak{v} \rangle^*, \text{ w. z. b. w.}$$

Anmerkung. Aus Satz 4 können leicht folgende Tatsachen erschlossen werden: Jede Lösung ω_{i1} der Gleichung $\sum_i a_i x_i^2 = a_1$ läßt sich zu einer Substitution $x_i = \sum_i \omega_{ik} y_k$ ergänzen, die die Form $\sum_i a_i x_i^2$ festläßt. Ebenfalls jede Lösung ω_{i1}, ω_{i2} des Gleichungssystems

$$\sum_i a_i x_{i1}^2 = a_1, \quad \sum_i a_i x_{i2}^2 = a_2, \quad \sum_i a_i x_{i1} x_{i2} = 0. \quad \text{Usw.}$$

Sind f und g zwei quadratische Formen, und sind die Variablen der einen Form unabhängig von den Variablen der anderen, so bilden wir die Summe $f + g$. Satz 4 können wir dann auch so aussprechen:

Aus $f_1 + f_3 \cong f_2 + f_3$ *darf* $f_1 \cong f_2$ *geschlossen werden.*

Für die Klassifikation der quadratischen Formen lehrt der folgende Satz, daß es nur auf die Kenntnis derjenigen Formen ankommt, welche die Null nicht darstellen (Grundformen). Angewandt auf den Körper P der reellen Zahlen ergibt sich beispielsweise sofort, daß der Trägheitsindex einer quadratischen Form invariant bleibt bei allen Transformationen.

Satz 5. *Stellt f die Null dar, so kann f auf die Gestalt $x^2 - y^2 + f'$ transformiert werden. Die Form f' ist (nach Satz 4) durch f bis auf Äquivalenz eindeutig bestimmt.*

Beweis. Es sei $\mathfrak{u}^2 = 0$, $\mathfrak{u} \neq 0$. Da $\mathfrak{R}$ kein Radikal besitzt, gibt es einen Vektor $\mathfrak{v}$ mit $\mathfrak{u}\mathfrak{v} = 1$. Für $\mathfrak{u}$, $\mathfrak{v}$ lautet die Produkttafel $\begin{pmatrix} 0 & 1 \\ 1 & * \end{pmatrix}$, diese Vektoren spannen also einen zweidimensionalen Raum $\mathfrak{r}$ mit $|\mathfrak{r}| \neq 0$ auf. Es gilt $\mathfrak{R} = \mathfrak{r} + \mathfrak{r}^*$, dabei hat $\mathfrak{r}$ nach dem Hilfssatz die Metrik $x^2 - y^2$.

Möglicherweise stellt auch f' die Null dar, dann ist

$$f' \cong x'^2 - y'^2 + f'', \qquad f \cong (x^2 - y^2) + (x'^2 - y'^2) + f''.$$

Auch die Form f'' ist durch f bis auf Äquivalenz eindeutig festgelegt.

Spalten wir von f möglichst oft Formen der Gestalt $X^2 - Y^2$ ab, so gelangen wir entweder zur leeren Form 0 oder zu einer Form, die nicht mehr die Null darstellt. Diese Form nennen wir die **Grundform** von f. Sie ist bis auf Äquivalenz durch f eindeutig bestimmt.

Zur Aufstellung aller Klassen äquivalenter Formen genügt daher die Angabe aller Klassen äquivalenter Grundformen.

Wenn f und g äquivalente Grundformen haben, so sagen wir, f und g sind **ähnlich**, $f \sim g$. Haben die Diagonalformen f und g die Koeffizienten a_i bzw. b_k, so erklären wir die **Summe** $f + g$ und das **Produkt** $f \cdot g$ durch die Diagonalformen mit den Koeffizienten a_i, b_k bzw. $a_i b_k$.

Es gilt $f - f \sim 0$, denn diese Form hat die Koeffizienten a_i, $-a_i$, und nach dem Hilfssatz kann jedes Paar a_i, $-a_i$ durch 1, -1 ersetzt werden. Wie jetzt leicht zu sehen ist, gilt

Satz 6. *Die Klassen ähnlicher Formen bilden einen Ring.*

Merkwürdig ist die Parallele zwischen quadratischen Formen und den normalen einfachen Algebren. Die Grundformen entsprechen den Schiefkörpern. In beiden Fällen führt die Einteilung in „ähnliche" Objekte zu einer Gruppe. Vermutlich besteht die Analogie noch in einem weiteren Umfange; so wäre es wünschenswert, zu beweisen, *daß eine Grundform auch in jedem Oberkörper von ungeradem Grad m die Null nicht darstellen kann.*

Ist bei festem Oberkörper $\overline{K}$ diese Vermutung für alle Formen mit $n \leqq m$ richtig, so läßt sie sich auch für jede Form f mit $n > m$ beweisen: Die Grundform f gehöre zum Raum $\mathfrak{R}$. Durch Erweiterung des Koeffizientenbereichs zu $\overline{K}$ entstehe der Raum $\overline{\mathfrak{R}}$. Ist $f = 0$ in $\overline{K}$ lösbar, so gibt es in $\overline{\mathfrak{R}}$ einen Vektor $\bar{\mathfrak{u}} \neq 0$ mit $\bar{\mathfrak{u}}^2 = 0$. Wegen $n > m$ ist $\bar{\mathfrak{u}}\mathfrak{v} = 0$ mit $\mathfrak{v} \neq 0$ aus $\mathfrak{R}$ lösbar. Da f Grundform ist, folgt $\mathfrak{v}^2 \neq 0$; $\bar{\mathfrak{u}}$ liegt im $(n-1)$-dimensionalen Raum $\overline{\langle \mathfrak{v} \rangle^*}$. Dies ist aber ein Widerspruch, wenn die Vermutung schon bis $n-1$ bewiesen ist.

Aus den allgemeinen Kriterien der Nulldarstellbarkeit (Abschnitt II) folgt die *Richtigkeit der Vermutung für*

$$n = 1, 2, 3, 4 \text{ und jedes ungerade } m,$$

nach der soeben gemachten Bemerkung folgt die Gültigkeit außerdem für

$$m = 3 \text{ und jedes } n.$$

Zum Nachweis, daß irgendein Ausdruck, der von den Koeffizienten einer Diagonalform $f = \Sigma a_i x_i^2$ abhängt, bei jeder Transformation (in andere Diagonalformen) invariant

bleibt, kann der Satz 7 dienlich sein. Wird eine binäre Teilform $a_i x_i^2 + a_k x_k^2$ in $a_i' x_i'^2 + a_k' x_k'^2$ transformiert, so ist damit auch eine Umformung von f in eine Diagonalform f' gegeben.

Satz 7. *Zwei äquivalente Diagonalformen f und g lassen sich immer derartig durch mehrmalige binäre Transformation ineinander überführen, daß jeweils die Diagonalgestalt bestehen bleibt.*

Beweis. Erstens sei f eine Grundform. Bekanntlich läßt sich jede Transformation aus Elementartransformationen zusammensetzen. D. h. jede Form läßt sich in eine äquivalente Form dadurch überführen, daß auf die Matrix der Form die folgenden Operationen wiederholt angewandt werden:

a) Vertauschung zweier benachbarter Zeilen,

b) Multiplikation einer Zeile mit einer Zahl,

c) Addition einer vervielfachten Zeile zu einer späteren,

jedesmal verbunden mit einer entsprechenden Umformung auf die Spalten. Bei einer derartigen allmählichen Transformation von f in g mögen die Matrizen $A_1, \ldots, A_s$ auftreten; dabei brauchen nur A_1 und A_s Diagonalmatrizen zu sein. Da f nicht die Null darstellt, läßt sich Satz 2 auf jede Matrix A_j anwenden, und wir gelangen dadurch zu einer äquivalenten Diagonalform f_j. A_j und A_{j+1} unterscheiden sich höchstens in einer der Teildeterminanten des Satzes 2, f_j und f_{j+1} unterscheiden sich daher höchstens in zwei Koeffizienten. Nach Satz 4 läßt sich f_j schon durch Transformation einer binären Teilform in f_{j+1} überführen. Wegen $f_1 = f$, $f_s = g$ ist die Behauptung für Grundformen bewiesen.

Zweitens stelle f die Null dar. f habe die Koeffizienten $a_1, a_2, a_3, \ldots$. Nach Satz 5 kann f in eine Form h mit den Koeffizienten $1, -1, c_3, \ldots$ transformiert werden. Wegen Satz 3 kann h binär in $a_1, -a_1, c_3, \ldots$ verwandelt werden. Die Behauptung sei schon für Formen mit weniger Variablen bewiesen. Nach Satz 4 ist $-a_1, c_3, \ldots \cong a_2, a_3, \ldots$, die Überführung kann durch mehrmalige binäre Transformation geschehen. Daher läßt sich f und ebenso g in der gewünschten Weise in h überführen. Damit ist die ganze Behauptung bewiesen.

Zu einem festen quadratischen Oberkörper K_2/K können *hermitesche Formen*

$$\sum_{i,k} a_{ik} x_i \bar{x}_k \qquad (a_{ik} = \overline{a_{ki}} \text{ aus } K_2)$$

eingeführt werden. *Alle Sätze dieses Abschnittes lassen sich* ohne Schwierigkeit auch *auf hermitesche Formen übertragen.* (Die Diskriminante $|a_{ik}|$ multipliziert sich hier bei Transformation mit der Norm einer Zahl aus K_2).

II. Die Systeminvariante $S(f)$ einer quadratischen Form.

Weitere Ergebnisse über quadratische Formen $f = \sum_{i=1}^{n} a_i x_i^2$ aus einem beliebigen Grundkörper K können wir gewinnen, wenn wir jeder solchen Form ein gewisses assoziatives hyperkomplexes System zuordnen.

Das Cliffordsche Zahlsystem $C(f)$ hat die Basis

$$u_1^{\nu_1} u_2^{\nu_2} \cdots u_n^{\nu_n} \qquad (\nu_i = 0, 1)$$

vom Rang 2^n und die Rechentafel

$$u_i^2 = a_i, \quad u_i u_k = -u_k u_i \qquad (i \neq k).$$

Die Rechenvorschrift können wir auch in eine einzige Regel zusammenfassen:

$$(\Sigma x_i u_i)^2 = \Sigma a_i x_i^2 = f.$$

Satz 8. *Zu äquivalenten Diagonalformen gehören isomorphe Cliffordsche Zahlsysteme.*

Beweis. f werde durch die Substitution $x_\alpha = \Sigma p_{\alpha\beta} \overline{x}_\beta$ in eine andere Diagonalform $\overline{f} = \Sigma \overline{a}_i \overline{x}_i^2$ übergeführt. $C(f)$ wird auch durch die Größen $\overline{u}_\beta = \Sigma u_\alpha p_{\alpha\beta}$ erzeugt. Wegen $\Sigma \overline{x}_i \overline{u}_i = \Sigma x_i u_i$ und $\Sigma a_i x_i^2 = \Sigma \overline{a}_i \overline{x}_i^2$ gilt

$$(\Sigma \overline{x}_i \overline{u}_i)^2 = \Sigma \overline{a}_i \overline{x}_i^2 = \overline{f}.$$

Da diese Gleichung genau so aussieht, wie die Rechenvorschrift für das System $C(\overline{f})$, ist $C(f) \cong C(\overline{f})$.

Das System $C(a_1 x_1^2 + a_2 x_2^2)$ wird in der Algebrentheorie gewöhnlich mit (a_1, a_2) bezeichnet; es ist einfach und hat den Grundkörper K als Zentrum. Für eine Form f mit ungerader Variablenzahl braucht das Cliffordsche System nicht mehr einfach zu sein. Aus diesem Grunde werden wir jetzt jeder Form f ein anderes invariantes System $S(f)$ zuordnen; dabei wird $S(f)$ direktes Produkt von mehreren Systemen der Gestalt (a, b) sein, also auch selbst einfach und normal sein.

Wir setzen $S(f) = C(F_n)$, wobei $F_n = f - \sum_{i=1}^{n} x_{-i}^2$ eine Form mit $2n$ Variablen ist, so daß $S(f)$ den Rang 4^n hat. Es ist nach Satz 8 klar, daß sich $S(f)$ nicht ändert bei Transformationen von f. Wir beweisen nun

Satz 9. $S(f) = \prod_{k=1}^{n} (d_k, a_k), \quad d_k = a_1 \cdots a_k.$

$C(F_n)$ wird von den Größen $u_1, u_{-1}, \ldots, u_n, u_{-n}$ erzeugt. Wegen $u_i^2 = a_i \neq 0$ sind dies keine Nullteiler. Wir setzen

$$v_1 = (u_1 u_{-1})(u_2 u_{-2}) \cdots (u_{n-1} u_{1-n})(u_n), \qquad v_2 = u_n u_{-n}.$$

Es ist $v_2 = a_n$. Um v_1^2 zu berechnen, beachten wir, daß die einzelnen Klammern, aus denen v_1 zusammengesetzt ist, untereinander vertauschbar sind. So folgt $v_1^2 = a_1 a_2 \cdots a_n = d_n$, ferner gilt $v_1 v_2 = -v_2 v_1$. v_1, v_2 erzeugen also ein Untersystem (d_n, a_n) vom Rang 4. Die mit v_1 und v_2 vertauschbaren Größen $u_1, u_{-1}, \ldots, u_{n-1}, u_{1-n}$ erzeugen ein anderes Untersystem $C(F_{n-1})$ vom Rang 4^{n-1}. Beide Systeme erzeugen zusammen $C(F_n)$. Mithin ist $C(F_n) = C(F_{n-1}) \times (d_n, a_n)$, aus dieser Rekursionsformel ergibt sich die behauptete Zerlegung von $S(f)$.

Bemerkung. Das Cliffordsche Zahlsystem $C(f)$ läßt sich für eine quadratische Form $\Sigma a_{ik} x_i x_k$ auch dann invariant definieren, wenn die Matrix a_{ik} nicht Diagonalgestalt hat: $u_1, \ldots, u_n$ seien assoziative, unvertauschbare Unbestimmte mit der definierenden Relation

$$(\Sigma x_i u_i)(\Sigma y_k u_k) = \Sigma a_{ik} x_i y_k,$$

d. h.

$$u_i u_k + u_k u_i = 2 a_{ik}.$$

Werden die 2^n linear unabhängigen Produkte der u_i mit U_I bezeichnet, so sind die Komponenten P_{IK}^L der Multiplikationstafel $U_I U_K = \sum_L P_{IK}^L U_L$ Polynome in den Koeffizienten a_{ik}.

Ähnlich wie in Satz 9 läßt sich auch $C(f)$ in Faktoren zerlegen, und zwar spaltet sich bei geradem n ein Faktor vom Rang 4, bei ungeradem n einer vom Rang 2 ab. Diese Faktoren sind jedoch komplizierter gebaut, überdies haben wir nachgeprüft, daß $C(f)$

schon von $S(f)$ und der Diskrimante d abhängt, so daß ein näheres Eingehen auf das System $C(f)$ unnötig ist.

Im Sinne der Algebrenähnlichkeit gelten, wie bekannt, folgende Regeln:

$$(a, c)\,(b, c) \sim (ab, c), \quad (b, a) \sim (a, b), \quad (a, -a) \sim 1 \quad \text{(Zerfall)}.$$

Auf Grund dieser Regeln finden wir für $S(f)$ die Zerlegungen

$$S(f) \sim \prod_{i \leq k} (a_i, a_k) \sim \prod_k (-d_{k-1}, d_k).$$

Nach einer kleinen Rechnung folgt

Satz 10. *Es gilt*

$$S(mf) \sim (m, (-1)^{\frac{n(n+1)}{2}} d^{n+1})\, S(f),$$
$$S(f+g) \sim (d(f), d(g))\, S(f)\, S(g).$$

Aus $d(f+g) \cong d(f+h)$ *und* $S(f+g) \sim S(f+h)$ *folgt* $d(g) \cong d(h)$ *und* $S(g) \sim S(h)$.

Im allgemeinen bilden d und S kein vollständiges Invariantensystem für die Äquivalenz quadratischer Formen. Z. B. haben für $n = 4$ die beiden Formen f und $-df$ stets gleiche Invarianten d und S, und trotzdem brauchen f und $-df$ nicht äquivalent zu sein, man betrachte etwa $f = \sum_1^4 x_i^2$ im Körper der reellen Zahlen.

Satz 11. *Für* $n = 1, 2, 3$ *sind* d *und* S *ein vollständiges Invariantensystem für Äquivalenz quadratischer Formen.*

Beweis. Für $n = 1$ ist d die einzige Invariante.

Für $n = 2$ seien $f = a x^2 + b y^2$ und $\bar{f} = \bar{a}\bar{x}^2 + \bar{b}\bar{y}^2$ zwei Formen mit gleichen Invarianten d und S. Wegen $S(f) \sim (-1, d)\,(a, b)$ und $S(\bar{f}) \sim (-1, d)\,(\bar{a}, \bar{b})$ ist $(a, b) \cong (\bar{a}, \bar{b})$, daher sind die Normenformen dieser Algebren

$$z_0^2 - a z_1^2 - b z_2^2 + ab z_3^2 \quad \text{und} \quad \bar{z}_0^2 - \bar{a}\bar{z}_1^2 - \bar{b}\bar{z}_2^2 + \bar{a}\bar{b}\bar{z}_3^2 \qquad (ab = \bar{a}\bar{b} = d)$$

einander äquivalent. Nach Satz 4 folgt daraus die Äquivalenz von f mit $\bar{f}$.

Für $n = 3$ seien $f = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2$ und $\bar{f}$ zwei Formen mit gleichen Invarianten d und S. Eine leichte Rechnung ergibt

$$s(f) = (-a_1 a_2, -a_1 a_3) \sim (-1, -1)\, S(f) \qquad (\text{für } n = 3).$$

Es ist also $(-a_1 a_2, -a_1 a_3) \cong (-\bar{a}_1\bar{a}_2, -\bar{a}_1\bar{a}_3)$, daher sind die mit $d = a_1 a_2 a_3 = \bar{a}_1\bar{a}_2\bar{a}_3$ multiplizierten Normenformen dieser Algebren

$$d z_0^2 + a_3 z_1^2 + a_2 z_2^2 + a_1 z_3^2 \quad \text{und} \quad d\bar{z}_0^2 + \bar{a}_3\bar{z}_1^2 + \bar{a}_2\bar{z}_2^2 + \bar{a}_1\bar{z}_3^2$$

einander äquivalent. Nach Satz 4 folgt daraus wieder $f \cong \bar{f}$.

Anwendung *auf solche Körper* k, *in denen jede Algebra* (a, b) *zerfällt.* **Beispiele** sind:

Ein Galoisfeld (nach dem Satz von Wedderburn);

ein algebraischer *Funktionenkörper* einer Variablen *mit algebraisch abgeschlossenem Konstantenkörper* (nach Tsen (6));

der reelle Funktionenkörper $\mathsf{P}(x, \sqrt{-1 - x^2})$ und dessen endliche Erweiterungen (Witt (8)).

Satz 12. *In solchen Körpern* K *sind* n *und* d *die einzigen Invarianten für die Äquivalenz quadratischer Formen.*

Beweis. Die Behauptung stimmt für $n = 1$ und nach Satz 11 auch für $n = 2$. Es sei $n > 2$ und die Behauptung bis $n - 1$ bewiesen. Dann ist

$$a_1, a_2, a_3, \ldots, a_n \cong 1, a_1 a_2, a_3, \ldots, a_n \cong 1, 1, 1, \ldots, d.$$

K sei wieder ein beliebiger Körper. Nach Satz 5 kann jede die Null darstellende Form f auf die Gestalt $x^2 - y^2 - dz^2$ gebracht werden, es folgt $s(f) \sim 1$. Aus Satz 11 folgt, daß umgekehrt eine Form f mit $s(f) \sim 1$ in $x^2 - y^2 - dz^2$ transformiert werden kann, mithin $f = 0$ lösbar ist:

Satz 13. *Für die Lösbarkeit von* $f = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 = 0$ *ist die Bedingung* $(-1, -1)\, S(f) \sim (-a_1 a_2, -a_1 a_3) \sim 1$ *notwendig und auch hinreichend.*

Für $n = 4$ beweisen wir

Satz 14. *Für die Lösbarkeit von* $f = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 + a_4 x_4^2 = 0$ *ist notwendig und auch hinreichend, daß die Algebra* $(-a_1 a_2, -a_1 a_4)$ *im Oberkörper* $K(\sqrt{d})$ *zerfällt.*

Wir setzen $-a_1 a_2 = a$, $-a_1 a_3 = b$, $a_1 a_2 a_3 = c$, $a_1 a_2 a_3 a_4 = d$. Im Oberkörper $K(\sqrt{d})$ wird $d \cong 1$, also wird

$$cf \cong dx_4^2 - ax_3^2 - bx_2^2 + abx_1^2$$

Normenform der Algebra (a, b). $f = 0$ in $K(\sqrt{d})$ ist daher gleichbedeutend mit $(a, b) \sim 1$ in $K(\sqrt{d})$. Aus $f = 0$ in K folgt erst recht $f = 0$ in $K(\sqrt{d})$, aber es ist auch der umgekehrte Schluß richtig: Sei $K(\sqrt{d}) > K$, d. h. $d \neq 1$ in K. Wenn dann $K(\sqrt{d})$ Zerfällungskörper von (a, b) ist, muß nach der allgemeinen Algebrentheorie ein zu $K(\sqrt{d})$ isomorpher Körper in (a, b) vorkommen, d muß also das Quadrat eines Elements $x_0 + x_3 u + x_2 v + x_1 uv$ aus (a, b) sein. Daraus folgt $x_0 = 0$ und $d = ax_3^2 + bx_2^2 - abx_1^2$, mithin ist $cf = 0$ auch in K lösbar. Satz 14 ist damit bewiesen.

In K braucht (a, b) keine Invariante von f zu sein, dagegen folgt nach leichter Rechnung die Invarianz im Oberkörper $K(\sqrt{d})$ wegen

$$(-a_1 a_2, -a_1 a_3) \sim (-1, -1)\, S(f) \text{ in } K(\sqrt{d}) \qquad (\text{für } n = 4),$$

indem wieder $d \cong 1$ in $K(\sqrt{d})$ beachtet wird.

Den Inhalt der Sätze 11, 13, 14 stellen wir in einer Tabelle zusammen:

n	Volles Invariantensystem für Äquivalenz	Bedingung für die Darstellbarkeit der Null
1	d	unmöglich
2	d und S	$d \cong -1$
3	d und S	$S \sim (-1, -1)$
4	?	$S \sim (-1, -1)$ in $K(\sqrt{d})$

Bemerkung (vgl. (4)). K enthalte mehr als 5 Elemente. Es seien $a, b, x \neq 0$, dann läßt sich t so wählen, daß $bt^2 \neq \pm a, 0$ wird, und es folgt

$$a \cdot x^2 + b \cdot 0^2 = a\left(x\frac{bt^2 - a}{bt^2 + a}\right)^2 + b\left(\frac{2axt}{bt^2 + a}\right)^2,$$

worin die neuen Quadrate nicht verschwinden. Durch Wiederholung dieses Verfahrens kann eine Lösung $x_1, \ldots, x_n$ von $f = 0$ (nicht alle $x_i = 0$) stets durch eine andere Lösung $y_1, \ldots, y_n$ ersetzt werden, in der sogar *alle* $y_i \neq 0$ sind.

Satz 15. *Darstellbarkeit einer Zahl* $m \neq 0$ *durch eine Form* f *ist gleichwertig mit der Lösbarkeit von* $f - mx^2 = 0$.

Denn jede Lösung von $f = m$ liefert eine Lösung von $f - mx^2 = 0$; ist umgekehrt $f - mx^2 = 0$ lösbar, so gibt es auch eine Lösung mit $x \neq 0$, sogar mit $x = 1$, also ist $f = m$ lösbar. Dasselbe gilt auch in den Körpern von 3 oder 5 Elementen, da für $n > 1$ jede Form f sämtliche Zahlen $m \neq 0$ darstellt.

Anwendung auf einen $\mathfrak{p}$-adischen Zahlkörper ($\mathfrak{p}$ endlich):

Satz 16. *In einem $\mathfrak{p}$-adischen Zahlkörper stellt jede quinäre quadratische Form die Null dar (also auch jede Form mit $n \geqq 5$).*

Zum Beweis werde angenommen, daß $f = 0$ unlösbar ist. Dies trifft dann auch zu für die Teilform a_1, a_2, a_3, a_4 von $df = a_1, a_2, a_3, a_4, a_5$. Nach Satz 14 ist $K(\sqrt{a_1 a_2 a_3 a_4})$ kein Zerfällungskörper von $(-a_1 a_2, -a_1 a_3)$. Im $\mathfrak{p}$-adischen wird bekanntlich eine Algebra (a, b) von jedem quadratischen Oberkörper zerfällt, also ist $a_1 a_2 a_3 a_4 \cong 1$ oder $a_5 \cong 1$. Entsprechend folgt $a_i \cong 1$, also $df \cong \sum_1^5 x_i^2$. Weiter ist $(-a_1 a_2, -a_1 a_3) = (-1, -1) \nsim 1$, das ergibt $\mathfrak{p} \mid 2$. In diesem Fall liegt $\sqrt{-7}$ in K und es ist $1^2 + 1^2 + 1^2 + 2^2 + \sqrt{-7}^2 = 0$, $df = 0$ ist doch lösbar, w. z. b. w.

Anwendung *auf solche Körper K, in denen jede quinäre quadratische Form die Null darstellt.* **Beispiele** sind:

Ein $\mathfrak{p}$-adischer Zahlkörper für endliches $\mathfrak{p}$ (Satz 16);

ein algebraischer *Funktionenkörper* einer Variablen *mit endlich vielen Konstanten* (nach Chevalley (**1**) (**7**) und Tsen (**6**));

ein algebraischer *Funktionenkörper in zwei Variablen mit algebraisch abgeschlossenem Konstantenkörper* (Tsen (**6**)).

Satz 17. *In solchen Körpern K sind n, d und S ein volles Invariantensystem für die Äquivalenz von quadratischen Formen.*

Beweis. Für $n = 1, 2, 3$ war das schon gezeigt. Es sei $n > 3$ und die Behauptung bis $n - 1$ bewiesen. f und $\bar{f}$ seien zwei Formen mit gleichen Invarianten d und S. Wir setzen $f = ax^2 + h$. Nach Voraussetzung ist $\bar{f} = a$ lösbar, daher kann nach Satz 1 die Form $\bar{f}$ auf die Gestalt $a\bar{x}^2 + \bar{h}$ gebracht werden. Aus Satz 10 folgt $d(h) \cong d(\bar{h})$ und $S(h) \sim S(\bar{h})$. Wegen der Induktion ist $h \cong \bar{h}$, folglich $f \cong \bar{f}$.

Es wird jetzt noch gezeigt, welche Algebren S auftreten können als Invarianten von quadratischen Formen f mit vorgegebener Variablenanzahl $n > 1$ und vorgegebener Diskriminante d.

Satz 18. *Für $n = 2$ und vorgegebenem d treten genau diejenigen S auf, für die $S \sim (-1, -1)$ in $K(\sqrt{-d})$ ist.*

Wird über den Körper K die einschränkende Voraussetzung gemacht, daß alle Algebren (a, b) eine Gruppe bilden, so treten die Invarianten $n \geqq 3$, d und $S \sim (a, b)$ in beliebiger Zusammenstellung wirklich auf.

Beweis. Für die Form $ax^2 + by^2$ ist $(-1, -1)S \sim (-a, -d)$, also $S \sim (-1, -1)$ in $K(\sqrt{-d})$. Wird dies umgekehrt über S vorausgesetzt, so läßt sich $(-1, -1)S$ in der Gestalt $(-a, -d)$ schreiben, und die Form $ax^2 + ady^2$ hat die Invarianten d und S. $n \geqq 3$, d und (a, b) seien vorgelegt. Nach Voraussetzung dürfen wir $(-1, -1)(a, b) \sim (p, q)$ setzen. Für

$$g = dpqx_1^2 - dqx_2^2 - dpx_3^2$$

ist dann $s(g) = (p, q)$, also $S(g) \sim (a, b)$. $f = g + \sum_{i=4}^{n} x_i^2$ ist also eine Form mit den Invarianten n, d und $S \sim (a, b)$.

Beispiele *von Körpern, in denen die Algebren (a, b) eine Gruppe bilden:*

Zahlkörper,

$\mathfrak{p}$-adische Körper,

algebraische Funktionenkörper einer Variablen mit endlich vielen Konstanten.

III. Quadratische Formen in speziellen Körpern.

Für einen $\mathfrak{p}$-*adischen Körper* ($\mathfrak{p}$ endlich) oder einen
algebraischen Funktionenkörper über einem Galoisfeld
geben die Sätze 17 und 18 eine klare Übersicht über die Klassen äquivalenter Formen: n, d und S sind ein vollständiges Invariantensystem, und für $n \geqq 3$ sind d und S unabhängig. Im Falle $n \geqq 5$ stellt jede Form die Null dar, für $n = 1, 2, 3, 4$ ist die Bedingung für die Lösbarkeit von $f = 0$ auf der allgemeingültigen Tabelle auf S. 39 angegeben.

Im Falle des *Körpers der reellen Zahlen* sind der Rang n und der Trägheitsindex j (Anzahl der negativen Quadrate) ein vollständiges Invariantensystem, und zwischen ihnen besteht die einzige Relation $0 \leqq j \leqq n$. Die Bedingung für die Lösbarkeit von $f = 0$ lautet: $0 < j < n$.

Das Ziel in diesem Abschnitt ist, eine entsprechende Übersicht zu gewinnen für
1. *Zahlkörper*,
2. *reelle Funktionenkörper einer Variablen.*

1. Zahlkörper.

Aus der Zahlkörpertheorie sind für uns folgende Tatsachen grundlegend:

(1) Wenn eine Zahl an allen Primstellen $\mathfrak{p}$ (d. h. in allen $\mathfrak{p}$-adischen Oberkörpern) Quadratzahl ist, so ist sie schlechthin (d. h. im Zahlkörper K) Quadratzahl.

(2) Wenn eine Algebra (a, b) an allen Primstellen zerfällt, so zerfällt (a, b) schlechthin.

(3) Die Anzahl der Stellen, an denen (a, b) nicht zerfällt, ist gerade.

(4) Die Algebren (a, b) bilden eine Gruppe.

Für den Beweis des nachfolgenden Satzes bemerken wir:

(5) Im Falle einer ternären Form ist $f = 0$ an einer geraden Anzahl von Stellen unlösbar. Dies folgt aus (3) und Satz 13.

(6) Ist $\mathfrak{p}$ endlich und kein Teiler von 2, und sind mindestens drei Koeffizienten einer Diagonalform f prim zu $\mathfrak{p}$, so stellt f an der Stelle $\mathfrak{p}$ die Null dar. Denn die Theorie der $\mathfrak{p}$-adischen Körper lehrt, daß an solchen Stellen $\mathfrak{p}$ eine Algebra (a, b) zerfällt, sobald $\mathfrak{p}$ prim ist zu a und b; nach Satz 13 enthält die Form f also eine ternäre Teilform, welche die Null darstellt.

Satz 19. *Wenn $f = 0$ an allen Stellen lösbar ist, so auch im Zahlkörper K.*

Beweis. Für $n = 1, 2, 3, 4$ folgt die Nulldarstellbarkeit in K aus der Tabelle auf S. 39 in Verbindung mit (1) und (2).

Nun sei $n \geqq 5$. Wir setzen $f = \varphi - \psi$, wobei φ $n - 2$ und ψ zwei Variable enthält. $\mathfrak{p}_i$ durchlaufe erstens alle Primideale, die in den Koeffizienten von f vorkommen, zweitens alle Primfaktoren von 2, drittens alle unendlichen Stellen. Bei der Nulldarstellung von f in $k_{\mathfrak{p}_i}$ mögen φ und ψ den Wert μ_i annehmen. Sollte $\mu_i = 0$ sein, so stellen φ und ψ alle Zahlen dar, wir dürfen daher $\mu_i \neq 0$ annehmen. In folgender Weise approximieren wir jetzt die endlich vielen μ_i durch ein einziges μ aus dem Zahlkörper K:

In $\mathfrak{p}_i^e$ werde der Exponent e so hoch gewählt, daß der Strahl mod $\mathfrak{p}_i^e$ aus lauter $\mathfrak{p}_i$-adischen Quadratzahlen besteht. Ist $\mathfrak{p}_i^{a_i}$ der genaue Beitrag zu μ_i an der endlichen Stelle $\mathfrak{p}_i$, so wählen wir eine Hilfszahl ϱ mit

$$(\varrho) = \mathfrak{a} \prod_{\text{endl.}} \mathfrak{p}_i^{a_i}, \qquad (\mathfrak{a}, \mathfrak{p}_i) = 1.$$

Nach dem Satz von der arithmetischen Progression gibt es ein Primideal $\mathfrak{q}$ mit

$$\mathfrak{q} = \mathfrak{a}\xi, \qquad \xi \equiv \frac{\mu_i}{\varrho} \bmod \mathfrak{p}_i^e.$$

Wird jetzt $\mu = \varrho\xi$ gesetzt, so folgt

$$(\mu) = \mathfrak{q} \prod_{\text{endl.}} \mathfrak{p}_i^{a_i}, \qquad \mu \equiv \mu_i \bmod \mathfrak{p}_i^{e}.$$

Wir zeigen jetzt, daß die Formen φ und ψ an allen Stellen die Zahl μ darstellen. Für $\mathfrak{p} = \mathfrak{p}_i$ ist dies der Fall, da an diesen Stellen $\mu \cong \mu_i$ ist.

Wegen (6) stellt die Form $\varphi - \mu x^2$ an den Stellen $\mathfrak{p} \neq \mathfrak{p}_i$, und falls außerdem $\mathfrak{p} \neq \mathfrak{q}$ ist, auch die Form $\psi - \mu y^2$ die Null dar. Für die restliche Stelle $\mathfrak{q}$ muß $\psi - \mu y^2 = 0$ nach (5) lösbar sein.

Da die Formen $\varphi - \mu x^2$ und $\psi - \mu y^2$ weniger als n Variablen enthalten, und an allen Stellen die Null darstellen, dürfen wir für sie die Nulldarstellbarkeit in K schon annehmen. Wenn aber φ und ψ beide in K die Zahl μ darstellen, so ist $f = \varphi - \psi = 0$ in K lösbar, q. e. d.

Satz 20. *Wenn an allen Stellen $f \sim 0$ ist oder wenn überall $f \cong g$ ist, so gilt das entsprechende schlechthin im Körper K.*

Beweis durch Induktion nach n. Es sei $n > 0$, und überall $f \sim 0$. Nach Satz 19 ist $f = 0$ in K lösbar, d. h. nach Satz 5 ist $f \sim f'$ in K $(n' < n)$. Weil an allen Stellen $f' \sim 0$ ist, gilt im Körper K: $f' \sim 0$ und damit $f \sim 0$. — Wenn f und g gleichviel Variable enthalten, so ist die Aussage $f \cong g$ gleichwertig mit $f - g \sim 0$.

Die Sätze 19 und 20 ermöglichen uns, die Theorie der quadratischen Formen im Großen (d. h. im Zahlkörper K) zurückzuführen auf die schon hergeleitete Theorie im Kleinen (d. h. in den $\mathfrak{p}$-adischen Körpern, Sätze 16 und 17).

Mit j_ν bezeichnen wir den Trägheitsindex einer Form f an der reellen unendlichen Erweiterung K_ν. Werden die neuen Ergebnisse in die Tabelle auf S. 39 aufgenommen, so erhalten wir die beiden ersten Spalten der folgenden

Tabelle für einen Zahlkörper K.

n	Volles Invariantensystem für Äquivalenz	Bedingungen für die Darstellbarkeit der Null	Einzige Relationen zwischen den angegebenen Invarianten
1	d	unmöglich	keine
2	d und S	$d \cong -1$	$S \sim (-1, -1)$ in $K(\sqrt{-d})$
3	d und S	$S \sim (-1, -1)$	keine
4	d, S, j_ν	$S \cong (-1, -1)$ in $K(\sqrt{d})$	$d \cong (-1)^{j_\nu}$ und $S \sim (-1, -1)^{\frac{j_\nu(j_\nu+1)}{2}}$ in K_ν $(0 \leqq j_\nu \leqq n)$.
5, 6, usw.	d, S, j_ν	$0 < j_\nu < n$	

Es ist noch die letzte Tabellenspalte nachzuprüfen: Für $n = 2, 3$ ist Satz 18 maßgebend. Wie ferner eine leichte Rechnung ergibt, gelten die Relationen

$$(n) \qquad d \cong (-1)^{j_\nu} \quad \text{und} \quad S \sim (-1, -1)^{\frac{j_\nu(j_\nu+1)}{2}} \quad \text{in } K_\nu \qquad (0 \leqq j_\nu \leqq n)$$

sicher für jedes n. Für $n = 3$ folgt allein aus diesen Relationen, daß j_ν nur von d und S abhängt.

Es sei $n \geqq 4$. Wir beweisen jetzt induktiv, daß außer den Relationen (n) keine weiteren bestehen zwischen den Invarianten d, S, j_ν, indem wir zeigen:

Satz 21. *Wenn zwischen gegebenen d, S, j_ν die Relationen (n) bestehen, so gibt es eine quadratische Form f mit diesen Invarianten $(n \geqq 4)$.*

Zu diesem Zweck werde

$$\iota_v = \begin{cases} 0 & \text{falls} \quad j_v \neq n \\ 1 & \text{falls} \quad j_v = n \end{cases}$$

eingeführt. In K werde eine Zahl δ mit dem K_v-Vorzeichen $(-1)^{\iota_v}$ bestimmt. Aus den angenommenen Relationen (n) für n, d, S, j_v folgen nach leichter Umformung die entsprechenden Relationen $(n-1)$ für die Größen

$$d' = d\delta, \quad S' = S \cdot (\delta, d), \quad j_v' = j_v - \iota_v.$$

Im Fall $n - 1 = 3$ sei f' eine Form mit den Invarianten d' und S'. Wie schon gesagt, hat dann f' von selbst die Trägheitsindizes j_v. Falls $n - 1 > 3$, gibt es nach Induktionsvoraussetzung eine Form f' zu d', S', j_v'.

Aus Satz 9 folgt jetzt, daß die Form $f = \delta x^2 + f'$ in n Variablen gerade die Invarianten d, S, j_v hat, w. z. b. w.

2. Reeller Funktionenkörper.

Durch die Gleichung $F(x, y) = 0$ mit reellen Koeffizienten sei der reelle algebraische Funktionenkörper K definiert. Diejenigen Punkte $\mathfrak{p}$ auf der Riemannschen Fläche des Oberkörpers $K(i)$, in welchen sämtliche Funktionen α des Körpers K reelle Werte $\alpha(\mathfrak{p})$ annehmen, bilden eine Reihe von geschlossenen Kurven, die sich nicht schneiden. Diese „reellen Kurven" spielen eine entscheidende Rolle für die Untersuchung der Algebren über K. Aus der Arbeit (8) entnehmen wir die folgenden Tatsachen:

(1) Eine Algebra (α, β) zerfällt genau dann, wenn für fast alle Kurvenpunkte $\mathfrak{p}$ die Algebra $(\alpha(\mathfrak{p}), \beta(\mathfrak{p}))$ (über dem reellen Konstantenkörper) zerfällt, d. h. wenn fast nirgends α und β zugleich negativ werden.

(2) Wird jede Kurve in eine endliche Anzahl von Intervallen eingeteilt, und werden zu diesen Intervallen willkürliche Vorzeichen gewählt, so gibt es Funktionen, die in fast allen Kurvenpunkten genau das verlangte Vorzeichen annehmen.

Hierauf fußend behaupten wir folgende Sätze.

Satz 22. *Wenn für fast alle Kurvenpunkte* $\mathfrak{p}$ *die reelle quadratische Form* $f(\mathfrak{p}) = \sum_1^n \alpha_i(\mathfrak{p})\, x_i^2$ *indefinit ist, so stellt die Form* $f = \sum_1^n \alpha_i\, x_i^2$ *im Körper* K *die Null dar* $(n \geqq 3)$.

Beweis. Für $n = 3$ folgt die Behauptung aus Satz 13 in Verbindung mit (1). Für $n > 3$ wenden wir Induktion an. Wir setzen $f = \varphi - \psi$, wobei φ wieder $n - 2$ und ψ zwei Variable enthält. Nach (2) können wir eine Funktion μ wählen, die in fast allen Punkten positive Werte annimmt, in welchen entweder φ oder ψ positiv definit wird; dagegen soll μ in fast allen übrigen Kurvenpunkten negativ werden. Weil f in fast allen Punkten indefinit ist, sind nach dieser Wahl von μ auch die beiden Formen $\varphi - \mu x^2$ und $\psi - \mu y^2$ in fast allen Punkten indefinit, sie stellen mithin nach Induktion beide im Körper K die Null dar. Wenn aber φ und ψ beide die Zahl μ darstellen, ist $f = \varphi - \psi = 0$ in K lösbar.

Den Trägheitsindex von $f(\mathfrak{p}) = \Sigma \alpha_i(\mathfrak{p}) x_i^2$ nennen wir den Trägheitsindex von $f = \Sigma \alpha_i x_i^2$ im reellen Kurvenpunkt $\mathfrak{p}$. Der Trägheitsindex werde jedoch nicht erklärt für die Nullstellen und Pole der α_i, er ist also nur in fast allen Punkten festgelegt.

Satz 23. *Wenn die Formen* f *und* g *in* n *Variablen dieselbe Diskriminante und in fast allen Kurvenpunkten gleichen Trägheitsindex haben, so sind* f *und* g *äquivalente Formen.*

Beweis. Die Form $h = f - g$ in $2n$ Variablen hat die Diskriminante $(-1)^n$ und den Trägheitsindex n. Durch Induktion zeigen wir die (mit $f \cong g$ gleichwertige) Behauptung $h \sim 0$:

Für $n = 1$ ist klar, daß $h = 0$ lösbar ist, und für $n > 1$ folgt die Nulldarstellbarkeit aus Satz 22. Nach Satz 5 ist $h \cong x^2 - y^2 + h'$, wo also h' eine Form in $2n - 2$ Variablen mit der Diskriminante $(-1)^{n-1}$ ist, die an fast allen Punkten den Trägheitsindex $n - 1$ hat. Folglich ist $h' \sim 0$ und damit auch $h \sim 0$.

Für die Diskriminante einer Form gilt an fast allen Kurvenpunkten $\operatorname{sign} d = (-1)^j$, wo j den Trägheitsindex in diesem Punkt bedeutet ($0 \leqq j \leqq n$).

Der folgende Satz lehrt, daß außer diesen angegebenen Relationen keine weiteren zwischen den Invarianten n, d, j bestehen.

Satz 24. *Man teile die reellen Kurven in endlich viele Intervalle* $[\nu]$ *ein und gebe* j_ν ($0 \leqq j_\nu \leqq n$) *und* d *aus* K *so vor, daß* $\operatorname{sign}_\nu d = (-1)^{j_\nu}$ *in fast allen Punkten gilt. Dann gibt es eine quadratische Form* f *in* n *Variablen mit der Diskriminante* d, *die in fast allen Punkten des Intervalls* $[\nu]$ *den Trägheitsindex* j_ν *besitzt.*

Beweis. Wir bestimmen nach (2) n Funktionen α so, daß im Intervall $[\nu]$

$$\alpha_1, \ldots, \alpha_{j_\nu} < 0 \quad \text{und} \quad \alpha_{j_\nu+1}, \ldots, \alpha_n > 0$$

ist. Dann hat

$$f = d\alpha_2 \cdots \alpha_n x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_n x_n^2$$

die vorgeschriebenen Invarianten.

Göttingen, den 25. 1. 1936.

Literaturverzeichnis.

(1) C. Chevalley, Démonstration d'une hypothèse de M. Artin, Abh. Math. Sem. Hamburg **11** (1935), S. 73.

(2) W. K. Clifford, Applications of Graßmann's extensive algebra, Math. Papers, p. 271 = Am. Journ. of Math. **1** (1878), p. 350.

(3) H. Hasse, Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, Crelle **152** (1923), S. 129.

—, Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen, Crelle **152** (1923), S. 205.

—, Symmetrische Matrizen im Körper der rationalen Zahlen, Crelle **153** (1924), S. 12.

—, Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, Crelle **153** (1924), S. 113.

—, Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper, Crelle **153** (1924), S. 158.

(4) K. Hensel, Zahlentheorie (1913), S. 308.

(5) H. Minkowski, Über die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Koeffizienten rational ineinander transformiert werden können, Ges. Abh. **1** (1914), S. 219.

(6) Ch. C. Tsen, Divisionsalgebren über Funktionenkörpern, Gött. Nachr. 1933, S. 335.

—, Algebren über Funktionenkörpern, Diss. Göttingen 1934.

(7) E. Warning, Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, Abh. Math. Sem. Hamburg **11** (1935), S. 76.

(8) E. Witt, Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Funktionenkörper, Crelle **171** (1934), S. 4.

Eingegangen 2. Mai 1936.

Über affektlose Gleichungen.

Von *Ph. Vassiliou* in Saloniki.

1. Eine kürzlich erschienene Arbeit von van der Waerden [1]), betreffend die Zerlegungs- und die Trägheitsgruppe eines Primideals im Galoisschen Wurzelkörper einer algebraischen Gleichung, erlaubt es uns, einige ältere Sätze über affektlose Gleichungen, sowie manche neue Konstruktion solcher Gleichungen, in überaus einfacher Weise zu erhalten.

Der in der genannten Arbeit von van der Waerden aufgestellte Hauptsatz stellt eine Verallgemeinerung eines bekannten Satzes von Artin[2]) dar; er vermittelt auch für den Fall eines Diskriminantenteilers den Zusammenhang, der zwischen der Primidealzerlegung in einem algebraischen Körper und den Zerlegungs- und Trägheitssubstitutionen der zugehörigen Galoisschen Gruppe besteht. Zu seiner Formulierung gehen wir gleich über.

2. Es seien $x_1, \ldots, x_n$ die voneinander verschiedenen Wurzeln einer algebraischen Gleichung $F(x) = 0$ im Grundkörper P (einem Zahl- oder Funktionenkörper), Ω der zugehörige Galoissche Wurzelkörper $\mathsf{P}(x_1, \ldots, x_n)$. Die Galoissche Gruppe von $F(x) = 0$ ist eine Gruppe von Permutationen dieser Wurzeln. Außerdem zerfalle im Körper $\mathsf{P}(x_1)$ das Primideal p des Grundkörpers P folgendermaßen:

$$p = \mathfrak{p}_{f_1}^{e_1} \mathfrak{p}_{f_2}^{e_2} \cdots \mathfrak{p}_{f_\varrho}^{e_\varrho},$$

also in ϱ verschiedene Primideale $\mathfrak{p}_{f_j}$ von den Graden f_j und den Exponenten e_j.

Für die Zerlegungsgruppe $\mathfrak{Z}$ und die Trägheitsgruppe $\mathfrak{T}$ (betrachtet als Permutationsgruppen) eines Primteilers $\mathfrak{P}$ von p in Ω sagt dann der genannte Satz folgendes aus:

Hilfssatz 1. *Die Wurzeln $x_1, \ldots, x_n$ zerfallen gegenüber $\mathfrak{Z}$ in ϱ Transitivitätsgebiete zu je $e_j f_j$ Wurzeln und gegenüber $\mathfrak{T}$ in f_j Transitivitätsgebiete zu je e_j Wurzeln.*

3. Wir beschränken uns jetzt auf den Fall des rationalen Grundkörpers R und nehmen an,

$$F(x) = x^n + a_1 x^{n-1} + \cdots + a_n \tag{1}$$

sei in R irreduzibel (die a_i gewöhnliche ganze Zahlen).

Wir machen ferner die Voraussetzungen, daß für die Primzahl p eine Kongruenz der Form:

$$F(x) \equiv x^h f(x) \pmod{p} \tag{2}$$

---

[1]) B. L. van der Waerden, Die Zerlegungs- und die Trägheitsgruppe als Permutationsgruppen, Math. Annalen **111** (1935), 731.

[2]) E. Artin, Über die Zetafunktionen gewisser algebraischer Zahlkörper, Math. Ann. **89** (1923), oder H. Hasse, Zahlbericht, Teil II, Jahresbericht D. M.-V., Ergänzungsband VI (1930), 126.

mit $h > 1$ besteht, und daß die Diskriminante Δ_1 des Polynoms $f(x)$ zu p teilerfremd ist. Letzteres bedingt, daß in der Primfunktionzerlegung von $f(x)$ mod. p alle Primfunktionen in der ersten Potenz aufgehen.

Es bezeichne weiter Δ die Diskriminante von $F(x)$, D die Diskriminante des Körpers $R(x_1)$ und d den sogenannten Index der Zahl x_1; die Relation, welche diese drei Zahlen verbindet, lautet bekanntlich

$$\Delta = d^2 D.$$

Wir wenden nun ein Kriterium von Dedekind an [3]), das uns erlaubt zu entscheiden, ob die Primzahl p ein Teiler des Index d ist, und das folgenden Wortlaut hat:

Hilfssatz 2. *Ist*

$$F(x) = f_1(x)^{e_1} f_2(x)^{e_2} \cdots f_\varrho(x)^{e_\varrho} + p\, M(x)$$

($f_j(x)$ *die verschiedenen Primfunktionen von* $F(x)$ *in der Zerlegung* mod. p), *so ist die Primzahl* p *dann und nur dann ein Teiler des Index, wenn das Polynom* $M(x)$ mod. p *durch eine der Primfunktionen* $f_j(x)$ *mit* $e_j > 1$ *teilbar ist.*

Infolge der angenommenen Voraussetzung $(\Delta_1, p) = 1$ und wegen dieses Satzes von Dedekind ist p kein Teiler von d, sobald a_n, welches gemäß (2) ja $\equiv 0$ (mod. p) ist, $\not\equiv 0$ (mod. p^2) ist. Setzt man also $\mathfrak{p}_1 = (p, x_1)$, so ist $\mathfrak{p}_1$ Primideal ersten Grades des Körpers $R(x_1)$, und die Primzahl p zerfällt im Körper $R(x_1)$ folgendermaßen:

$$p = \mathfrak{p}_1^h \mathfrak{p}_{f_2} \cdots \mathfrak{p}_{f_\nu}\ ^{4}),$$

also derart, daß nur das Primideal $\mathfrak{p}_1$ in einer höheren als der ersten Potenz aufgeht.

Wenn nun $(h, p) = 1$ wäre, so wäre die Diskriminante D höchstens durch die $(h-1)$-te Potenz der Primzahl p teilbar [5]). Nehmen wir also weiter an, daß die Primzahl p mindestens in der n-ten Potenz in der Diskriminante Δ von $F(x)$ aufgeht, was wegen $(d, p) = 1$ gleichbedeutend damit ist, daß D mindestens die n-te Potenz von p enthält, so müssen wir den Schluß ziehen, daß h durch p teilbar ist.

Nach dem unter **2** formulierten Satze von van der Waerden, nämlich wegen der darin behaupteten Transitivität der Trägheitsgruppe $\mathfrak{T}$ als Gruppe von h Wurzeln, ist die Ordnung der Galoisschen Gruppe unserer Gleichung (1) durch h und folglich dann durch p teilbar.

Zusammenfassend haben wir damit folgenden Satz von I. Schur [6]):

Satz 1. *Hat man eine im Körper der rationalen Zahlen irreduzible ganzzahlige Gleichung* (1) *vom Grade* n, *deren Diskriminante die Primzahl* p *mindestens in der* n*-ten Potenz enthält, und bei der das konstante Glied* a_n *durch* p, *aber nicht durch* p^2 *teilbar ist, besteht ferner eine Kongruenz der Form* (2), *wo* $h > 1$ *und die Diskriminante des Polynoms* $f(x)$ *zu* p *teilerfremd ist, so besitzt die Galoissche Gruppe der Gleichung eine durch* p *teilbare Ordnung.*

4. Genau von denselben Schlüssen ausgehend, kann man, unter Heranziehung von bekannten Sätzen über Permutationsgruppen, ebenso leicht verschiedene Klassen von affektlosen Gleichungen oder solchen mit alternierender Gruppe angeben.

Dazu benötigen wir noch den

---

[3]) R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Göttinger Abhandlungen 1878, § 3.

[4]) Siehe Weber-Fricke, Algebra III, 57.

[5]) Siehe Weber-Fricke, l. c. 119.

[6]) I. Schur, Gleichungen ohne Affekt, Sitz.Berichte Akad. Berlin 1930, 443—449.

Hilfssatz 3. *Sind in der Primidealzerlegung*

$$p = \mathfrak{p}_{f_1}^{e_1} \cdots \mathfrak{p}_{f_\varrho}^{e_\varrho}$$

alle Exponenten zu p teilerfremd, so ist die Verzweigungsgruppe von $\mathfrak{P}$ *in* Ω *gleich der Einheit.*

Zum Beweise dieser Tatsache verweisen wir auf einen kürzlich erschienenen Aufsatz von U. Wegner [7]).

5. Wir sind jetzt in der Lage, folgenden Satz zu beweisen:

Satz 2. *Hat man eine im Körper der rationalen Zahlen irreduzible ganzzahlige Gleichung* (1) *ungeraden Grades n, sind alle Koeffizienten* a_j *außer dem ersten* a_1 *durch eine Primzahl* $p > n$ *teilbar, insbesondere der letzte genau durch* p^1, *sind ferner für eine von p verschiedene Primzahl* $q > n$ *alle Koeffizienten außer den beiden ersten* a_1, a_2 *durch* q^2 *teilbar, insbesondere der letzte genau durch* q^1, *und ist* $a_1^2 - 4a_2 \equiv 0 \pmod{q^2}$, *so besitzt die Gleichung* (1) *die symmetrische Gruppe als Galoissche Gruppe.*

Beweis. Wegen der angenommenen Teilbarkeit der Koeffizienten durch p besteht die Kongruenz

$$F(x) \equiv x^{n-1}(x + a_1) \pmod{p},$$

und p ist nach Hilfssatz 2 kein Indexteiler. Folglich zerfällt p im Körper $R(x_1)$ folgendermaßen:

$$p = \mathfrak{p}_1^{n-1}\mathfrak{p}_1', \tag{3}$$

wo

$$\mathfrak{p}_1 = (p, x_1), \quad \mathfrak{p}_1' = (p, x_1 + a_1),$$

und die voneinander verschiedenen Primideale $\mathfrak{p}_1$, $\mathfrak{p}_1'$ sind beide vom ersten Grad. Gemäß der Voraussetzung $p > n$ sind die Exponenten in der Zerlegung (3) zu p teilerfremd; folglich ist nach Hilfssatz 3 die Verzweigungsgruppe eines Primteilers $\mathfrak{P}$ von p in Ω gleich der Einheit, und nach Hilfssatz 1 enthält die Galoissche Gruppe von $F(x)$ einen $(n-1)$-gliedrigen Zyklus.

Ebenso folgt aus den Voraussetzungen des Satzes über q, daß die Zerlegung von q im Körper $R(x_1)$ folgendermaßen lautet:

$$q = \mathfrak{q}_1^{n-2}\mathfrak{q}_1'^2,$$

und daß q nach Hilfssatz 2 kein Indexteiler ist. Nach Hilfssatz 3 und 1 folgt dann wieder die Existenz des Produktes eines $(n-2)$-gliedrigen und eines zweigliedrigen Zyklus, also weil n ungerade ist, die Existenz eines zweigliedrigen Zyklus in der Galoisschen Gruppe von $F(x)$.

Da $F(x)$ als irreduzibel angenommen ist, so ist die Galoissche Gruppe transitiv, und weil sie einen $(n-1)$-gliedrigen und einen zweigliedrigen Zyklus enthält, ist sie die symmetrische Gruppe [8]).

6. Gleichungen mit den obigen Voraussetzungen kann man ersichtlich sehr leicht explizit angeben, wie das z. B. von O. Perron [9]) geschieht.

Was die Irreduzibilität des Polynoms $F(x)$ in der obigen Konstruktion betrifft, so können wir uns am einfachsten des Eisensteinschen Kriteriums bedienen, wie das bei Perron der Fall ist, oder die folgende Modifikation anwenden:

---

[7]) U. Wegner, Zur Theorie der affektlosen Gleichungen, Math. Ann. **111** (1935), 738.

[8]) Siehe z. B. B. L. van der Waerden, Moderne Algebra I, 191.

[9]) O. Perron, Algebra II, 2. Aufl., 220, Satz 111.

$F(x)$ vom Grade $n = p^\alpha$ (p Primzahl) ist irreduzibel, wenn alle Koeffizienten bis auf den letzten a_n durch p teilbar sind und

$$F(-a_n) \not\equiv 0 \pmod{p^2}$$

ist.

Beweis. Wenn $F(x)$ reduzibel wäre, so sei $F(x) = \varphi(x) \cdot \psi(x)$, wo $\varphi(x)$, $\psi(x)$ mindestens vom ersten Grade sind und nach dem Gaußschen Lemma ganze rationale Koeffizienten haben.

Nun ist aber

$$F(x) = \varphi(x)\ \psi(x) \equiv x^n + a_n \equiv (x + a_n)^n \pmod{p},$$

also wegen der Eindeutigkeit der Zerlegung mod. p

$$\varphi(x) \equiv (x + a_n)^\varrho \pmod{p}$$
$$\psi(x) \equiv (x + a_n)^\sigma \pmod{p},$$

mit $\varrho, \sigma \geqq 1$, $\varrho + \sigma = n$, d. h.

$$\varphi(-a_n) \equiv 0, \qquad \psi(-a_n) \equiv 0 \pmod{p},$$

und somit

$$F(-a_n) = \varphi(-a_n)\ \psi(-a_n) \equiv 0 \pmod{p^2},$$

gegen die Voraussetzung.

Derselbe Beweis überträgt sich ohne weiteres auf den Fall eines beliebigen Grundkörpers P statt R.

Eingegangen 3. Mai 1936.

Vollkommene Funktionalmittel und gewisse Kegelschnitteigenschaften.

Von *Georg Aumann* in München.

---

1. *Einleitung.* In der Theorie der Mittelwerte spielen die quasiarithmetischen Mittel eine bevorzugte Rolle [1] [2]). Sofern es sich um *analytische* Mittelwerte handelt, lassen sich die quasiarithmetischen Mittel durch eine Funktionalgleichnug charakterisieren, die für zwei Argumente folgendermaßen lautet:

$$m\big(m(x_1, m(x_1, x_2)),\ m(m(x_1, x_2), x_2)\big) = m(x_1, x_2). \tag{1}$$

Für *reelle* Mittel [3]) dürfte die allgemeine Auflösung der Gleichung (1) ziemliche Schwierigkeiten machen; man kann nämlich reelle Mittel angeben, die (1) erfüllen (allerdings nicht streng monoton sind), aber nicht quasiarithmetisch, d. h. nicht in der Form

$$m = \varphi^{-1}\left(\frac{\varphi(x_1) + \varphi(x_2)}{2}\right)$$

darstellbar sind, wobei $\varphi(x)$ eine in $a < x < b$ stetige streng monotone Funktion und φ^{-1} die Umkehrfunktion von φ bedeutet.

Nennt man ein Mittel $m(x_1, x_2)$ *vollkommen*, wenn es (1) befriedigt, so haben wir die Tatsache, *daß es vollkommene reelle Mittel gibt, die nicht quasiarithmetisch sind.* Solange man eine vollständige Antwort auf die Frage nach der allgemeinen Auflösung der Funktionalgleichung (1) für reelle Mittel nicht kennt, ist es angebracht, im Bereich der vollkommenen reellen Mittel zunächst einmal gewisse Teilklassen zu betrachten.

Im folgenden wollen wir uns mit reellen vollkommenen *Funktionalmitteln* $m(x_1, x_2)$ beschäftigen, d. h. mit Mittelwerten, wie sie dem Mittelwertsatz der Differentialrechnung,

$$f(x_1) - f(x_2) = (x_1 - x_2)\, f'(m),$$

oder dem verallgemeinerten Mittelwertsatz entspringen. Wir werden dabei voraussetzen, daß die Ableitung der Funktion $f(x)$ streng monoton ist. Die sich aus (1) für $f(x)$ ergebende Bedingung läßt mit Verwendung eines bekannten Satzes über die Differenzierbarkeitseigenschaften stetiger monotoner Funktionen auf beliebig oftmalige Differenzierbarkeit von $f(x)$ schließen und liefert dann für die Funktion $f(x)$ eine Differentialgleichung fünfter Ordnung, welche die Kurve $y = f(x)$ in einem (x, y)-Parallelkoordinatensystem als *Kegelschnitt* kennzeichnet. Damit sind alle möglichen vollkommenen, aber auch zugleich alle möglichen quasiarithmetischen Funktionalmittel bestimmt.

---

[1]) G. Aumann, Aufbau von Mittelwerten mehrerer Argumente. II. (Analytische Mittelwerte), Math. Ann. **111** (1935), S. 713—730.

[2]) Vgl. die Schlußbemerkung in: G. Aumann, Konvexe Funktionen und die Induktion bei Ungleichungen zwischen Mittelwerten, Sitz.Ber. Bay.Akad. d. Wiss. 1933, S. 414.

[3]) Siehe Definition l. c. [2]), S. 404.

Von Nr. **5** ab beschäftigen wir uns mit geometrischen Fragen. Die geometrische Deutung der Bedingung (1) liefert eine einfache *Tangenten-Sekanten-Schließeigenschaft*, die die Kegelschnitte unter allen streng konvexen glatten Kurven auszeichnet. Diese Schließeigenschaft ist Grenzfall einer Sekanten-Schließeigenschaft (*Viereckseigenschaft*): Liegen die Eckpunkte der Vierecke $ABCD$ und $A'B'C'D'$ auf einem glatten Teilbogen eines (eigentlichen oder ausgearteten) Kegelschnitts, und ist

$$AB \parallel A'B',\ BC \parallel B'C',\ CD \parallel C'D', \text{ dann ist auch } DA \parallel D'A'.$$

Diese Eigenschaft ist charakteristisch für die genannten Bogen, und zwar innerhalb der Gesamtheit aller ebenen zusammenhängenden Punktmengen.

Ersetzt man in der Viereckseigenschaft das Wort „Viereck" allgemein durch „Trapez", so ergibt sich eine *Trapezeigenschaft*. Es ist bemerkenswert, daß die Trapezeigenschaft allein die Kegelschnitte nicht mehr aus der Gesamtheit aller ebenen zusammenhängenden Punktmengen heraushebt, sondern auch bei gewissen anderen Punktmengen auftritt.

Im Verlauf unserer Untersuchungen beweisen wir eine leichte Verallgemeinerung eines Satzes von A. Marchaud [4]) über ebene zusammenhängende Punktmengen der linearen Ordnung zwei (Nr. **7**).

2. *Funktionalmittel.* Wir definieren: Die eindeutige stetige Funktion $m(t_1, t_2)$ heißt im Bereich $a < t_i < b$, $i = 1, 2$, ein *Funktionalmittel*, wenn es zwei Funktionen $\varphi(t)$ und $\psi(t)$ gibt, die im Intervall $a < t < b$ eindeutig und differenzierbar sind und die Eigenschaft haben, daß für $a < t_1 < t_2 < b$ die Gleichung

$$(2, 1) \qquad \begin{vmatrix} \varphi(t_1) - \varphi(t_2) & \varphi'(t_3) \\ \psi(t_1) - \psi(t_2) & \psi'(t_3) \end{vmatrix} = 0$$

im Intervall $a < t_3 < b$ nur die eine Lösung $t_3 = m(t_1, t_2)$ besitzt. Um die Herkunft von m auszudrücken, schreiben wir

$$m(t_1, t_2) = M_{\varphi,\psi}(t_1, t_2).$$

Die geometrische Deutung von (2, 1) ist bekanntlich die folgende: Wir betrachten die in der Parameterform

$$(2, 2) \qquad u = \varphi(t), \quad v = \psi(t)$$

in der (u, v)-Ebene dargestellte Kurve $\mathfrak{K}$. Die Gleichung (2, 1) besagt dann, daß die Kurvensehne (t_1) (t_2) parallel ist zur Kurventangente in (t_3). Aus der Voraussetzung, daß es nur einen solchen Punkt (t_3) geben soll, folgert man, daß $\mathfrak{K}$ eine streng konvexe glatte Kurve ist mit einer Gesamtkrümmung $\leqq \pi$. Es gibt daher eine affine Transformation mit nicht verschwindender Determinante,

$$\varphi_1(t) = a_1\varphi(t) + a_2\psi(t) + a_3,$$
$$\psi_1(t) = a_4\varphi(t) + a_5\psi(t) + a_6,$$

bei der $\psi_1(t)$ streng monoton ausfällt. Es ist

$$M_{\varphi_1,\psi_1}(t_1, t_2) \equiv M_{\varphi,\psi}(t_1, t_2).$$

Führt man nun den neuen Parameter

$$(2, 3) \qquad x = \psi_1(t)$$

mit der Umkehrung $t = \chi(x)$ ein, so wird $\varphi_1(t) = \varphi_1(\chi(x)) = f(x)$. Setzt man noch $f_0(x) \equiv x$, so ergibt sich schließlich:

$$M_{f,f_0}(x_1, x_2) = \psi_1\big(M_{\varphi,\psi}(\chi(x_1), \chi(x_2))\big);$$

---

[4]) A. Marchand, Sur les continus d'ordre borné, Acta Math. **55** (1930), S. 67—115; Satz auf S. 85.

M_{f,f_0} ist das Bildmittel von $M_{\varphi,\psi}$ vermöge der Abbildung (2, 3). Bedenken wir, daß das Bildmittel eines vollkommenen Mittels wieder vollkommen ist, so können wir uns auf Grund der vorausgehenden Überlegungen bei der Suche nach vollkommenen Funktionalmitteln auf Mittel der Form M_{f,f_0} beschränken.

3. *Differenzierbarkeit.* Sei $f(x)$ im Intervall $a < x < b$ eindeutig und differenzierbar, und $f'(x)$ streng monoton (und damit stetig). Für $x_1 \neq x_2$ setzen wir

$$\frac{f(x_1) - f(x_2)}{x_1 - x_2} = Q(x_1, x_2) \quad \text{und} \quad \frac{\partial}{\partial x_1} Q(x_1, x_2) = R(x_1, x_2).$$

Da die Kurve $y = f(x)$ streng konvex ist, d. h. keine Strecke als Teil enthält, so gilt:

$$R(x_1, x_2) \neq 0 \quad \text{für} \quad x_1 \neq x_2.$$

Das Mittel $M_{f,f_0}(x_1, x_2) = m(x_1, x_2)$, definiert durch die Gleichung

$$Q(x_1, x_2) = f'(m),$$

sei als vollkommen vorausgesetzt. Es besteht dann das folgende Induktionsschema:

Aus den Gleichungen

$$(3, 1) \qquad Q(x_1, x_2) = f'(m),$$
$$(3, 2) \qquad Q(x_1, m) = f'(u_1),$$
$$(3, 3) \qquad Q(x_2, m) = f'(u_2)$$

folgt

$$(3, 4) \qquad Q(u_1, u_2) = f'(m).$$

Wir werden nun zeigen, daß $f''(x)$ vorhanden ist für jedes x, allgemeiner, daß $f(x)$ beliebig oft differenzierbar ist. In der Tat:

Da $f'(x)$ streng monoton und stetig ist, so gibt es eine Stelle c in (a, b), an der $f''(c)$ vorhanden ist [5]). Man wähle ein festes m genügend nahe bei c, aber von c verschieden; u_1 variiere in einer Umgebung von c. Da $Q(x_1, x_2)$ in jeder einzelnen Veränderlichen streng monoton ist, so folgt aus (3, 2) $x_1 = x_1(u_1)$, aus (3,1) dann $x_2 = x_2(u_1)$, und aus (3,3) dann $u_2 = u_2(u_1)$. Die Funktionen $x_1(u_1)$, $x_2(u_1)$ und $u_2(u_1)$ sind stetig und streng monoton, außerdem sind die x_1, x_2, u_1, u_2, m alle voneinander verschieden. Lassen wir nun u_1 gegen c streben! Aus (3,2), (3,1), (3,4) und (3,3) ergeben sich dann die Gleichungen:

$$x_1'(c) = \frac{f''(c)}{R(x_1(c), m)},$$
$$x_2'(c) = -\frac{R(x_1(c), x_2(c))}{R(x_2(c), x_1(c))} x_1'(c),$$
$$u_2'(c) = -\frac{R(c, u_2(c))}{R(u_2(c), c)},$$
$$f''(u_2(c))\, u_2'(c) = R(x_2(c), m)\, x_2'(c),$$

gleichgültig, ob $f''(c)$ endlich ist oder nicht. Wir finden also:

$$(3, 5) \qquad f''(u_2) = \frac{R(u_2, c)\, R(x_1, x_2)\, R(x_2, m)}{R(c, u_2)\, R(x_2, x_1)\, R(x_1, m)} f''(c)$$

für alle u_2 in einer gewissen Umgebung von c. $f(x)$ ist somit in einer ganzen Umgebung von c zweimal differenzierbar. Es kann $f''(c)$ weder 0 noch ∞ sein. Indem man jetzt in (3,5) m variieren läßt, schließt man in ähnlicher Weise wie eben auf beliebig oftmalige Differenzierbarkeit von $f(x)$ in einer Umgebung der Stelle c, und, indem man an Stelle von c nacheinander geeignete neue Punkte wählt, auf dieselbe im ganzen Intervall (a, b).

[5]) Siehe C. Carathéodory, Reelle Funktionen, Leipzig 1918, S. 573.

4. *Die vollkommenen Funktionalmittel.* Nachdem wir in **3** festgestellt haben, daß das $f(x)$ eines vollkommenen Mittels M_{f,f_0} beliebig oft differenzierbar ist, sind wir imstande, eine Differentialgleichung aufzustellen, der $f(x)$ notwendigerweise genügen muß. Am einfachsten gelingt dies, indem man bei festem m in den Gleichungen (3,1) bis (3,4) den Grenzübergang $x_1 \to m$ durchführt mit

$$f(m+h) = f(m) + f'(m)\,h + \cdots + \frac{f^{(5)}(m)}{5!}h^5 + \frac{h^6}{6!}f^{(6)}(m+\vartheta h).$$

Da die zugehörige Rechnung, wenn auch etwas lang, keine Schwierigkeiten bietet, so sei nur das Ergebnis genannt: Man erhält mit den Abkürzungen

$$\frac{f'''}{3f''} = \omega_1, \quad \frac{f^{(4)}}{6f''} = \omega_2, \quad \frac{f^{(5)}}{60f''} = \omega_3$$

die Differentialgleichung

$$2\omega_3 - 3\omega_2\omega_1 + 4\omega_1^3 = 0,$$

deren Integralkurven $y = f(x)$ in einer (x, y)-Ebene mit der Nebenbedingung $f'' \neq 0$ bekanntlich nicht ausgeartete Kegelschnitte darstellen.

Daß umgekehrt Funktionen $y = f(x)$, die eigentliche Kegelschnitte liefern, zu den gesuchten gehören, folgt daraus, daß die Mittel $M_{\varphi_i,\psi_i}(t_1, t_2)$, $i = 1, 2, 3$, mit

$$\begin{aligned}
&(4,1) && \varphi_1 = t, && \psi_1 = t^2, && \\
&(4,2) && \varphi_2 = \cos t, && \psi_2 = \sin t, && (0 < t < \pi) \\
&(4,3) && \varphi_3 = \operatorname{Cos} t, && \psi_3 = \operatorname{Sin} t &&
\end{aligned}$$

alle das arithmetische Mittel $\frac{t_1 + t_2}{2}$ darstellen, welches ja vollkommen ist. Mittels der in **2** beschriebenen Transformation erhält man aber aus (4,1), (4,2), (4,3) alle Kegelschnittbogen mit der Gleichung $y = f(x)$. Damit ist bewiesen:

Satz 1. *Das durch die reellen Funktionen $\varphi(t)$, $\psi(t)$ im Bereich $a < t_1, t_2 < b$ dargestellte Funktionalmittel $M_{\varphi,\psi}(t_1, t_2)$ ist dann und nur dann vollkommen, wenn der durch* (2,2) *dargestellte Kurvenbogen Teil eines nicht ausgearteten Kegelschnittes ist.*[6])

5. *Schließeigenschaften der Kegelschnitte.* Daß die in Satz 1 ausgesprochene Bedingung hinreichend ist, sieht man rascher als in **4** auf geometrischem Wege ein. Ist nämlich das Mittel $M_{\varphi,\psi}$ vollkommen, so hat die durch (2,2) dargestellte streng konvexe glatte Kurve $\mathfrak{K}$ folgende Eigenschaft (siehe Figur):

Eigenschaft A. Sind P_1, P_2 Punkte von $\mathfrak{K}$, ist weiter die Tangente in M an $\mathfrak{K}$ parallel zur Sehne P_1P_2, die Tangente in Q_i an $\mathfrak{K}$ parallel zur Sehne P_iM, $i = 1, 2$, so ist Q_1Q_2 parallel zu P_1P_2.

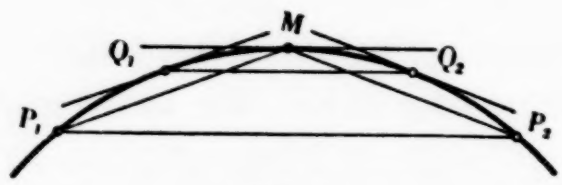

Fig. 1.

Man sieht sofort, daß die Eigenschaft A von der Parameterdarstellung der Kurve (vgl. **2**) unabhängig und gegenüber affinen Abbildungen invariant ist. Aus dieser letzten Bemerkung schließt man, daß jeder Teilbogen eines nicht ausgearteten Kegelschnitts

[6]) Wegen eines Beweises des analogen Satzes für quasiarithmetische Funktionalmittel, der sich nicht auf den hier mitgeteilten Beweis stützt, siehe G. Aumann, Über einen elementaren Zusammenhang zwischen Mittelwerten, Streckenrechnung und Kegelschnitten, Tôhoku Math. Journ. **42** (1936), S. 32—37.

die Eigenschaft A besitzt, weil ja die Kegelschnitte in jeder Richtung affine Symmetrie haben. Der geometrische Inhalt von Satz 1 ist also der

Satz 2. *Unter allen streng konvexen glatten Kurven mit einer Gesamtkrümmung* $\leqq \pi$ *sind die Teilbogen der nicht ausgearteten Kegelschnitte die einzigen, welche die Eigenschaft* A *besitzen.*

Die Eigenschaft A ist Grenzfall der folgenden stärkeren Eigenschaft:

Eigenschaft B. Sind P_1, P_2 und M_1, M_2 vier Punkte von $\mathfrak{K}$, wobei P_1P_2 parallel zu M_1M_2 ist, verläuft weiter die Tangente in Q_i an $\mathfrak{K}$ parallel zur Sehne P_iM_i, $i = 1, 2$, so ist Q_1Q_2 parallel zu P_1P_2.

Aus dem Grenzübergang $M_1 \to M \leftarrow M_2$, der bei einer streng konvexen glatten Kurve $\mathfrak{K}$ ohne weiteres ausführbar ist, folgt, daß die Eigenschaft B die Eigenschaft A nach sich zieht. Wegen der schon genannten Affinsymmetrie besitzen die Kegelschnitte die Eigenschaft B. Daher gilt der

Satz 3. *Unter allen streng konvexen glatten Kurven mit einer Gesamtkrümmung* $\leqq \pi$ *sind die Teilbogen der nicht ausgearteten Kegelschnitte die einzigen, welche die Eigenschaft* B *besitzen* [7]).

6. *Die Trapezeigenschaft.* Im folgenden heißen vier verschiedene Punkte A, B, C, D ein *Viereck*; ist dabei $AB \parallel CD$ oder $BC \parallel AD$, so heißt es ein *Trapez* [8]). Ist dann $\mathfrak{M}$ eine ebene Punktmenge, so definieren wir für $\mathfrak{M}$ folgendes als

Eigenschaft C (*Trapezeigenschaft*). Gehören die Ecken der zwei Trapeze $P_1M_1M_2P_2$ und $Q_1Q_1'Q_2'Q_2$ alle zu $\mathfrak{M}$, und ist $Q_1'Q_2' \parallel P_1P_2 \parallel M_1M_2 \parallel Q_1Q_2$, $Q_1Q_1' \parallel P_1M_1$, so ist auch $Q_2Q_2' \parallel P_2M_2$.

Aus dieser Definition geht ganz leicht hervor, *daß jede streng konvexe glatte Kurve mit der Eigenschaft* B *zugleich die Eigenschaft* C *besitzt, und umgekehrt.*

Bei einer allgemeinen Untersuchung der Punktmengen mit der Eigenschaft C erscheint es natürlich, allgemeinere Punktmengen als gerade glatte Kurven in die Betrachtung mit einzubeziehen. Wir beweisen den

Satz 4. *Jede ebene zusammenhängende Punktmenge* $\mathfrak{M}$ *mit der Eigenschaft* C *liegt entweder auf einem (eigentlichen oder ausgearteten) Kegelschnitt oder auf drei von einem Punkt ausgehenden Halbstrahlen, die solche Winkel gegeneinander bilden, daß jede beliebige Gerade mindestens einen Halbstrahl trifft* [9]).

Beweis (1. Teil). Wir betrachten den Fall, daß drei verschiedene Punkte von $\mathfrak{M}$, etwa A, B, C auf einer Geraden $\mathfrak{g}_0$ liegen. Jede von $\mathfrak{g}_0$ verschiedene, zu $\mathfrak{g}_0$ parallele Gerade $\mathfrak{g}$ trifft $\mathfrak{M}$ in höchstens einem Punkt. Gäbe es nämlich auf $\mathfrak{g}$ zwei verschiedene Punkte von $\mathfrak{M}$, etwa D und E, so würden die Trapeze $DABE$, $DACE$ der Eigenschaft C widersprechen. Gibt es außerhalb $\mathfrak{g}_0$ keinen Punkt von $\mathfrak{M}$, so ist wegen der Bedingung des Zusammenhängens von $\mathfrak{M}$ weiter nichts mehr zu beweisen.

Sei nun D ein Punkt außerhalb von $\mathfrak{g}_0$. Ich behaupte, daß dann der Durchschnitt $\mathfrak{J}_0$ von $\mathfrak{M}$ mit $\mathfrak{g}_0$ zusammenhängend ist. Angenommen, es gäbe einen nicht zu $\mathfrak{M}$ gehörigen

---

[7]) Dieser Satz läßt sich auch, ohne auf den Satz 2 und damit Satz 1 zurückgehen zu müssen, wie folgt, beweisen. Man benutze den Satz: Haben die streng konvexen differenzierbaren Funktionen $f_1(x)$, $f_2(x)$ ein gemeinsames Definitionsintervall, und gilt dort $M_{f_1,f_0} \equiv M_{f_2,f_0}$, so gilt dort $f_2(x) \equiv cf_1(x) + d$, wo c, d Konstanten sind. Für eine Kurve $\mathfrak{K}$ mit der Eigenschaft B folgert man aus diesem Satz, daß jedes Parallelenbüschel auf $\mathfrak{K}$ eine affine Selbstabbildung erzeugt. Diese Eigenschaft ist aber für die Kegelschnitte bekanntlich kennzeichnend.

[8]) Es ist zulässig, daß A, B, C, D in einer Geraden liegen.

[9]) Die Punktmenge $\mathfrak{M}$ heißt zusammenhängend, wenn für jede Zerlegung von $\mathfrak{M}$ in zwei fremde, nicht leere Summanden wenigstens ein Summand einen Häufungspunkt des anderen enthält.

Punkt P auf $\mathfrak{g}_0$, der zwischen den Punkten A und B liegt. Wir legen durch P die Gerade $\mathfrak{h}$ parallel zu AD. Auf $\mathfrak{h}$ liegen höchstens zwei Punkte von $\mathfrak{M}$; die Abstände dieser Punkte von $\mathfrak{g}_0$ seien $\geqq \delta > 0$. Nun schließen wir $\mathfrak{g}_0$ in zwei zu $\mathfrak{g}_0$ parallele Geraden $\mathfrak{g}_1$ und $\mathfrak{g}_2$ ein mit einem Abstand $\frac{\delta}{2}$ von $\mathfrak{g}_0$. Da $\mathfrak{g}_1$ und $\mathfrak{g}_2$ je höchstens einen Punkt mit $\mathfrak{M}$ gemein haben, so läßt sich ein, aus je einem Stück von $\mathfrak{g}_1$, $\mathfrak{h}$, $\mathfrak{g}_2$ zusammengesetzter, zu $\mathfrak{M}$ fremder Weg angeben, der A und B trennt, im Widerspruch damit, daß $\mathfrak{M}$ zusammenhängend ist. $\mathfrak{J}_0$ ist also ein lineares Intervall auf $\mathfrak{g}_0$. Sei nun $\mathfrak{h}_0$ irgendeine $\mathfrak{g}_0$ schneidende Gerade. Ich betrachte den Bereich der Ebene, der gebildet wird von allen zu $\mathfrak{h}_0$ parallelen, $\mathfrak{J}_0$ treffenden Geraden. Aus der Eigenschaft C folgt, daß je drei Punkte von $\mathfrak{M}$, die dem genannten Bereich, aber nicht $\mathfrak{g}_0$ angehören, auf einer Geraden liegen müssen.

Aus dem bisher Gesagten folgert man schließlich, daß $\mathfrak{M}$ entweder zusammenhängende Teilmenge eines sich schneidenden Geradenpaares ist oder auf drei von einem Punkt ausgehenden Halbstrahlen liegt, von denen jeder im erhabenen Winkelraum der beiden andern liegt.

7. *Satz über ebene zusammenhängende Punktmengen der linearen Ordnung zwei.* Ehe wir mit dem Beweis von Satz 4 fortfahren, zeigen wir:

Ist $\mathfrak{C}$ eine mehrpunktige zusammenhängende Punktmenge der Ebene, die von jeder Geraden in höchstens zwei Punkten getroffen wird, so ist $\mathfrak{C}$ eine streng konvexe einfache Kurve [10]).

Beweis. a) *Je vier verschiedene Punkte von $\mathfrak{C}$ bestimmen ein konvexes Viereck.* In der Tat: Angenommen, es gäbe vier verschiedene Punkte A, B, C, D von $\mathfrak{C}$, und D liege im Innern des Dreiecks ABC. A_1 sei der Schnittpunkt der Geraden AD mit BC, B_1 der von BD mit AC. A_1 und B_1 gehören nicht zu $\mathfrak{C}$. Ich behaupte nun, daß die Strecke A_1B_1 einen Punkt E von $\mathfrak{C}$ enthält. Wäre das nämlich nicht der Fall, so würde C von D durch den zu $\mathfrak{C}$ fremden Weg getrennt werden, welcher besteht aus der Strecke A_1B_1 und aus den beiden Halbgeraden, die von A_1 bzw. B_1 ausgehen, A bzw. B nicht enthalten und auf den Geraden AA_1 bzw. BB_1 liegen (Widerspruch!). Die Gerade CE trifft eine der Strecken DA_1, DB_1 im Innern, etwa DA_1 im Punkt F, der dann nicht zu $\mathfrak{C}$ gehören kann. Die von F ausgehenden, auf den Geraden CF bzw. AF liegenden, C bzw. A nicht enthaltenden Halbstrahlen bilden einen zu $\mathfrak{C}$ fremden Weg, der B und C trennt (Widerspruch!). Damit ist die obige Behauptung bewiesen.

b) Seien A, B, C drei verschiedene Punkte von $\mathfrak{C}$, und O ein Punkt im Innern des Dreiecks ABC. Jeder Halbstrahl $\mathfrak{s}$ durch O trifft $\mathfrak{C}$ in höchstens einem Punkt $P_{\mathfrak{s}}$; sonst gäbe es nämlich vier Punkte von $\mathfrak{C}$, die kein konvexes Viereck bildeten, im Widerspruch zu a). Würde $P_{\mathfrak{s}}$ mit $\mathfrak{s}$ nicht stetig variieren, so ließen sich zwei Punkte D, E von $\mathfrak{C}$ so finden, daß die Verlängerung der Strecke DE durch das Innere von ABC geht, was wieder zu a) im Widerspruch steht. Falls es zwei Halbstrahlen durch O gibt, die zu $\mathfrak{C}$ fremd sind, so enthält der von diesen beiden Halbstrahlen gebildete konvexe Winkelraum überhaupt keine Punkte von $\mathfrak{C}$, da sonst $\mathfrak{C}$ nicht zusammenhängen würde.

Aus a) und b) ergibt sich somit, daß $\mathfrak{C}$ eine streng konvexe einfache (offene oder geschlossene) Kurve darstellt.

8. *Fortsetzung des Beweises von Satz 4.* Wir haben noch den Fall zu untersuchen, wo $\mathfrak{M}$ von jeder Geraden in höchstens zwei Punkten geschnitten wird. Da in diesem

[10]) Dies ist etwas mehr als der Satz von A. Marchaud, l. c. [4]), weil wir in der Voraussetzung auf die Abgeschlossenheit von $\mathfrak{C}$ verzichten. Zudem ist unser Beweis denkbar elementar.

Fall $\mathfrak{M}$ nach **7** eine streng konvexe Kurve ist, haben wir, um den Anschluß an Satz 3 zu bekommen, nur noch zu zeigen, daß $\mathfrak{M}$ überall eine eindeutige Tangente besitzt.

Sei auf $\mathfrak{M}$ ein Durchlaufungssinn festgelegt; t_P^+ bzw. t_P^- bezeichne die vordere bzw. hintere Tangente im Punkt P von $\mathfrak{M}$ an $\mathfrak{M}$. Wir führen in der Eigenschaft C (vgl. **6**) folgenden Grenzübergang aus: Bei festen $P_1, P_2\ Q_1, Q_2$ mit $P_1P_2 \parallel Q_1Q_2$ lassen wir einseitig $M_1 \to P_1$, $M_2 \to P_2$ streben mit $M_1M_2 \parallel P_1P_2$. Dann strebt Q_i' mit $Q_iQ_i' \parallel M_iP_i$, $i = 1, 2$, gegen R_i. $\mathfrak{M}$ hat demnach die folgende Eigenschaft:

Es sei $R_1R_2 \parallel P_1P_2 \parallel Q_1Q_2$, $t_{P_1}^+ \parallel Q_1R_1$, dann ist $t_{P_2}^- \parallel Q_2R_2$.

Auf Grund dieser Eigenschaft können wir von $\mathfrak{M}$ unmittelbar behaupten: Sind P_1, P_2 zwei innere Punkte von $\mathfrak{M}$, so folgt aus $t_{P_1}^+ \parallel t_{P_1}^-$ stets $t_{P_2}^+ \parallel t_{P_2}^-$. Dies hat aber, da jede konvexe einfache Kurve mit Ausnahme von abzählbar vielen Punkten in jedem inneren Punkt eine eindeutige Tangente besitzt, zur Folge, daß $\mathfrak{M}$ in jedem inneren Punkt glatt ist. Damit ist der Beweis von Satz 4 fertig.

9. *Die Viereckseigenschaft.* Wir sahen, daß nicht jede ebene zusammenhängende Punktmenge mit der Eigenschaft C Teil eines Kegelschnitts sein muß. Durch Verschärfung der Eigenschaft C können wir aber die Kegelschnitte aussondern.

Man zeigt leicht, etwa an Hand der drei in **4** genannten Typen (oder mit Hilfe des Pascalschen Satzes), daß jeder Teilbogen $\mathfrak{M}$ eines eigentlichen Kegelschnitts die folgende Viereckseigenschaft hat:

Eigenschaft D. Sind A, B, C, D und A', B', C', D' zu $\mathfrak{M}$ gehörige Eckpunkte zweier Vierecke und ist $AB \parallel A'B'$, $BC \parallel B'C'$ und $CD \parallel C'D'$, so ist auch $DA \parallel D'A'$.

Diese Eigenschaft ist im wesentlichen charakteristisch für die genannten Punktmengen. Es gilt nämlich der

Satz 5. *Jede zusammenhängende ebene Punktmenge mit der Eigenschaft* D *ist Teil eines eigentlichen Kegelschnitts oder einer Geraden* [11]).

In der Tat, da D die Eigenschaft C nach sich zieht, so genügt es nach Satz 4 nur zu zeigen, daß eine Punktmenge $\mathfrak{M}$, die ein Geradenstück $\mathfrak{S}$ und einen außerhalb dieser Geraden gelegenen Punkt P enthält, die Eigenschaft D nicht besitzen kann. Sind A, B, C, D vier verschiedene Punkte auf $\mathfrak{S}$, so widersprechen die Vierecke $PABC$ und $PABD$ der Eigenschaft D.

Bemerkung. Der Viereckseigenschaft der Kegelschnitte entspricht in projektiver Fassung die

Eigenschaft E. Liegen die acht Ecken zweier Vierecke $ABCD$ und $A'B'C'D'$ auf einem Kegelschnitt und gehören die Schnittpunkte dreier Paare entsprechender Seiten einer und derselben Geraden an, so auch der Schnittpunkt des vierten Paares.

Setzt man darin $A' = B$, $B' = A$, so erhält man die Pascalsche Sechspunkteeigenschaft. Andererseits folgt durch zweimalige Anwendung der Pascalschen Sechspunkteeigenschaft die Achtpunkteeigenschaft E.

---

[11]) Statt dessen könnte man auch sagen: *glatter* Teilbogen eines (eigentlichen oder ausgearteten) Kegelschnitts.

Eingegangen 23. Mai 1936.

Zur Gaußschen Kompositionstheorie der binären quadratischen Formen.

Von *S. Lubelski* in Warschau.

Die Gaußsche Kompositionstheorie der binären quadratischen Formen verläuft bekanntlich parallel mit der Dedekind-Hilbertschen Idealklassentheorie quadratischer Körper [1]). Demnach scheint die erstere überflüssig zu sein. Doch ist sie als Beweismethode für die Theorie der binären quadratischen Formen $f(x, y)$ mit ganzen algebraischen Koeffizienten von Bedeutung. Sie gibt uns nämlich die Möglichkeit, in natürlicher und verhältnismäßig klarer Weise die Untergruppe g der gesamten Idealklassengruppe G, die durch $f(x, y)$ gebildet wird, hervorzuheben und oft die Ordnung H von g zu berechnen. In einer früheren Arbeit [2]) habe ich nämlich den folgenden Satz bewiesen:

Satz 1. *Es sei* $K(\sqrt{-q})$, $q \neq 2$ *Primzahl, ein imaginär-quadratischer Körper mit ungerader Klassenzahl,* $D > 2$ *eine natürliche Zahl, die für* $q = 1$ *größer als* 12 *ist und für welche* $D' = \frac{D}{4}$ *eine ganze, durch keine Quadratzahl des Körpers* $K(\sqrt{-q})$ *teilbare Zahl ist; ferner sei* h *die Klassenzahl der binären quadratischen Formen der Determinante* D, h' *die Klassenzahl der binären quadratischen Formen der Determinante* $-qD$ *im Körper der rationalen Zahlen. Dann gilt:*

Die Klassenzahl H *der binären quadratischen Formen der Determinante* D, *deren Koeffizienten ganze Zahlen des Körpers* $K(\sqrt{-q})$ *sind, ist* $H = \frac{hh'}{2}$ *für* $q \geqq 3$. *Ist* $q = 1$, *so ist* $H = hh'$ *oder* $2hh'$, *je nachdem* $x^2 - D'y^2 = -1$ *in ganzen rationalen Zahlen lösbar ist oder nicht.*

Die Herglotzsche Formel für die Ordnung H_1 von G ergibt für $D \geqq 12$

$$H_1 = \frac{hh'h_1}{2},$$

wo h_1 die Klassenzahl von $K(\sqrt{-q})$ bezeichnet [3]). Im Falle $h_1 = 1$ decken sich offenbar beide Formeln. Im allgemeinen sind sie aber wesentlich verschieden. Unsere Formel ist nämlich nur von *zwei* Parametern abhängig, die Herglotzsche dagegen von *drei*. In gewissen Fällen, z. B. für $(h_1, \frac{1}{2}hh') = 1$, erhält man mittels eines Furtwänglerschen

[1]) Dies war die Ursache dafür, daß man sich nicht mit der Gaußschen Kompositionstheorie beschäftigt hatte.

[2]) S. Lubelski, Über Klassenzahlrelationen quadratischer Formen in quadratischen Körpern, Journ. f. d. r. u. a. Math. **174** (1935), S. 160—184.

[3]) Man sieht also schon aus dieser Formel, wie auch aus Satz 1, daß unsere Bemerkung in [2]), S. 160: *die Klassenzahl* H *eines algebraischen Körpers . . ., der durch Zusammensetzung von* m *quadratischen Körpern* K_g $(g = 1, 2, \ldots, m)$ *entsteht . . ., ist durch das Produkt der Klassenzahlen* $h_1 h_2 \cdots h_m$ *teilbar,* offenbar bis auf einen Faktor $\frac{1}{2^t}$ gedacht ist.

Satzes (vgl. Satz 3 von [2])) aus einer Formel die andere. Um das Verhältnis der Formeln von H und H_1 ausführlich zu beleuchten, brauchen wir eine rein arithmetische Interpretation der Herglotzschen Formel, die wir nur für ungerades H_1 geben. Daraus erhalten wir in § 1 mit elementaren Mitteln einerseits eine Abschätzung der Herglotzschen Formel für relativ quadratische Körper mit ungerader Klassenzahl, andererseits Sätze über die *simultane Darstellbarkeit von rationalen Primzahlen durch binäre quadratische Formen.* Die genannten Formeln sind also für die Verteilung der Primzahlen von Bedeutung.

In § 2 geben wir auf Grund der Gaußschen Kompositionstheorie den (längst gesuchten) rein arithmetischen (also ohne Zuhilfenahme des Begriffes der reellen Zahl geführten) Beweis für die Existenz von nichttrivialen ganzen rationalen Lösungen der Pellschen Gleichung $x^2 - Dy^2 = 1$. Zugleich ergibt sich ein einfacher Beweis einer merkwürdigen Petrschen Verallgemeinerung des letzteren Satzes.

§ 1.

Satz 2. *Ist K ein über $K(\sqrt{-q})$ relativ quadratischer Körper, so entspricht jeder Idealklasse C aus K eindeutig ein System von drei ganzzahligen Formen $\{F_i\}$, deren Diskriminanten den Diskriminanten der quadratischen Unterkörper paarweise gleich sind. Sind C und $\bar{C}$ zwei Idealklassen, denen die Formensysteme $\{F_i\}$, $\{\bar{F}_i\}$ entsprechen, so entspricht dem Produkte $C\bar{C}$ das Formensystem $\{F_i\bar{F}_i\}$. Ist die Klassenzahl H_1 von K ungerade, so ist die genannte Zuordnung umkehrbar eindeutig.*

Beweis. Es seien $K(\sqrt{d_i})$ sämtliche quadratischen Körper, die zu K gehören, Δ_i ihre Diskriminanten. Ist j ein zur Idealklasse C von K gehöriges Ideal, so bilden die ganzen zu j und $K(\sqrt{d_i})$ gehörigen Zahlen ein Ideal j_i. Die ganzzahligen binären quadratischen Formen, die j_i entsprechen, ordnen wir der Idealklasse C zu. Nun ist $j_i = j s_i j$, wo $s_i j$ aus j nach Ausführung einer entsprechenden, eindeutig bestimmten Permutation s_i der galoisschen Gruppe von K entsteht. Sind also C und $\bar{C}$ zwei Idealklassen aus K, so entspricht der Idealklasse $C\bar{C}$ das Formensystem $\{F_i\bar{F}_i\}$, wenn nur $\{F_i\}$ bzw. $\{\bar{F}_i\}$ der Idealklasse C bzw. $\bar{C}$ entspricht. Mithin läßt sich die Eindeutigkeit der Zuordnung leicht beweisen. Denn sind j und $\bar{j}$ zwei zu C gehörige Ideale, so folgt aus $j = l\bar{j}$, wo l eine Zahl des Körpers K ist, daß $j(s_i j) = l(s_i l) \cdot \bar{j}(s_i \bar{j})$ ist, wo $l(s_i l)$ zu $K(\sqrt{d_i})$ gehört. Also gehören $j(s_i j)$ und $\bar{j}(s_i \bar{j})$ zu derselben Klasse von $K(\sqrt{d_i})$.

Schwieriger ist zu beweisen, ob die genannte Zuordnung eindeutig umkehrbar ist. Dazu müssen wir H_1 als ungerade voraussetzen. Sind nämlich C und $\bar{C}$ zwei Idealklassen, denen dasselbe System $\{F_i\}$ entspricht, so ergibt die Idealklasse $C\bar{C}^{-1}$ das Hauptsystem, d. h. das System, das aus den Hauptformen von $K(\sqrt{d_i})$ besteht. Bezeichnet $\mathfrak{a}$ ein beliebiges zu $\bar{C}C^{-1}$ gehöriges Ideal, so ergibt also $\mathfrak{a} s_i \mathfrak{a}$ eine Zahl aus $K(\sqrt{d_i})$. Demnach gehört $s_i \mathfrak{a}$ zur Klasse $\bar{C}^{-1}C$. Da $\mathfrak{a}(s_1\mathfrak{a})(s_2\mathfrak{a})(s_3\mathfrak{a}) = N(\mathfrak{a})$ ist, so ist $\bar{C}^{-1}C$ ambig und mithin $\bar{C}^{-1}C$ die Einheitsklasse, da H_1 ungerade ist.

Folgerung. *Die Anzahl H_1 der Idealklassen von K ist ein Teiler des Produktes der Idealklassen von $K(\sqrt{d_i})$, sofern H_1 ungerade ist.*

Der Beweis ergibt sich unmittelbar aus der Tatsache, daß sämtliche Systeme $\{F_i\}$ eine Gruppe $\mathfrak{G}$ bilden. Diejenigen Systeme, die den Idealklassen von K entsprechen, bilden also eine Untergruppe von $\mathfrak{G}$.

Satz 3. *Eine rationale Primzahl p sei durch die ganzzahligen Formen*

$$f(x, y) = ax^2 + bxy + cy^2, \quad f_1(x, y) = a_1x^2 + b_1xy + c_1y^2$$

gleichzeitig darstellbar. Die Diskriminanten $d = b^2 - 4ac$, $d_1 = b_1^2 - 4a_1c_1$ seien bis auf 4 quadratfrei, $(p, 4dd_1) = 1$, und die Klassenzahl H_1 von $K(\sqrt{d}, \sqrt{d_1})$ sei ungerade. Dann stellen die Formen $f(x, y)$, $f_1(x, y)$ unendlich viele Primzahlen dar, und die Menge dieser Primzahlen ist von positiver Dichte.

Beweis. Es bezeichne $\mathfrak{p}$ einen Primidealteiler von p und C die Klasse, zu der $\mathfrak{p}$ gehört. Offenbar ist p nach den Voraussetzungen des Satzes in $K(\sqrt{d})$ wie auch in $K(\sqrt{d_1})$ zerlegbar. Demnach ist $p = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, wo $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ Primideale ersten Grades sind. Der Klasse C, zu der $\mathfrak{p}$ gehört, entspricht also nach Satz 2 ein System von Formen, zu dem $f(x, y)$ und $f_1(x, y)$ gleichzeitig gehören. Nach einem Furtwänglerschen Satze enthält C unendlich viele Primideale ersten Grades, deren Normen nach Satz 2 durch die Formen $f(x, y)$, $f_1(x, y)$ gleichzeitig darstellbar sind. Nach dem Furtwänglerschen Satze beträgt die Dichte der Primzahlen ersten Grades, die zu C gehören, $\frac{1}{4H_1}$.

Folgerung. *Bei den Voraussetzungen der Sätze 1 und 2 ist die Anzahl der Systeme $\{F_i\}$ (wo F_1 eine Hauptform mit negativer Diskriminante bezeichnet), die gleichzeitig unendlich viele Primzahlen darstellen, $H = \frac{1}{2}\frac{H_1}{h_1}$* (dies ist also auch die Anzahl der Systeme, die keine in der Diskriminante von K nicht enthaltenen Primzahlen darstellen).

Beweis. Die Anzahl der Systeme $\{f_i\}$, die den Idealklassen nach Satz 1 und 2 entsprechen, beträgt $\frac{1}{2}\frac{H_1}{h_1} = H$. Die Formen dieser Systeme stellen also unendlich viele Primzahlen dar. Nun ist eine Form eines solchen Systems der Hauptform des imaginärquadratischen Körpers $K(\sqrt{-q})$ gleich.

Bemerkung. Der Satz 3 gibt uns die Möglichkeit, die Systeme $\{F_i\}$ effektiv aufzufinden, sogar allgemein. Z. B. ist im relativ quadratischen Körper $K(\sqrt{3}, \sqrt{-5})$ die Klassenzahl nach Herglotz gleich 2. Da

$$47 = 3 \cdot 3^2 + 5 \cdot 2^2 = 2 \cdot 2^2 + 2 \cdot 2 \cdot 3 + 3 \cdot 3^2$$

ist, so sind nur die Formensysteme

$$\{\pm(x^2 - 3y^2),\ x^2 + 5y^2,\ x^2 + 15y^2\}, \qquad \{\pm(x^2 - 3y^2),\ 2x^2 + 2xy + 3y^2,\ 3x^2 + 5y^2\}$$

möglich und nur diese stellen also gleichzeitig unendlich viele Primzahlen dar. Demnach ist die Anzahl der binären quadratischen Formen der Determinante 12 mit Koeffizienten aus dem Körper $K(\sqrt{-5})$ gleich 1.

Bemerkung. Aus den Sätzen 1, 2 und aus der Herglotzschen Formel erhält man leicht, daß $H_1 = \frac{hh'h_1}{2}$. Dagegen folgt dies allein aus der Herglotzschen Formel nicht unmittelbar.

§ 2.

Satz 4 (Arithmetischer Beweis der Lösbarkeit der Pellschen Gleichung). *Die Gleichung $x^2 - Dy^2 = 1$, wo D eine natürliche quadratfreie Zahl bezeichnet, ist in natürlichen Zahlen x, y lösbar.*

Beweis. I. Wäre die Gleichung

$$x^2 - Dy^2 = d, \quad d \mid D \tag{1}$$

in natürlichen Zahlen lösbar, so würde sich aus

$$dx_1 = x, \quad dx_1^2 - D_1 y^2 = 1, \qquad D_1 = \frac{D}{d},$$

die Gleichung

$$(dx_1^2 + D_1 y^2)^2 - D(2y^2 x_1^2)^2 = (dx_1^2 - D_1 y^2)^2 = 1$$

ergeben. Wir können also annehmen, daß auch die Gleichung (1) nicht lösbar ist.

II. Demnach kann man leicht eine untere Grenze für die Anzahl der ambigen Formen der Determinante $4D$ angeben. Nach einem Gaußschen Satze kann jede ambige Form in die Gestalt $ax^2 + a\varrho xy + cy^2$ $(\varrho = 0, 1)$ transformiert werden [4]). Sind die verschiedenen Formen

$$ax^2 + a\varrho\, xy + cy^2, \qquad a_1 x^2 + a_1 \varrho_1 xy + c_1 y^2 \qquad (\varrho, \varrho_1 = 0, 1)$$

der Determinante $4D$ zueinander äquivalent, so ist für gewisse ganze rationale Zahlen u, V

$$a_1 = au^2 + a\varrho u V + V^2, \quad aa_1 = U^2 - DV^2, \quad U = au + \frac{a\varrho}{2} V.$$

Da D quadratfrei ist, so muß $(a, a_1) | (U, V)$ sein. Mithin ist d durch $x^2 - Dy^2$ darstellbar, wobei $d = \frac{a a_1}{(a, a_1)^2}$, $d | D$ ist. Nach I ist dies nur dann möglich, wenn $a_1 = -\frac{DV^2}{a}$ ist. Zwei ambige Formen $ax^2 + a\varrho xy + cy^2$ mit positiven ersten Koeffizienten sind also nicht äquivalent, wenn nur $a \neq a_1$ ist. Nun erhalten wir für $\varrho = 1$ und $a = 2\bar{a}$

$$(2\bar{a})^2 - 4\,(2\bar{a})\,c = 4D,$$

also $\bar{a}^2 - 2\bar{a}c = D$. Da c ungerade ist, so muß gelten:

$$D \equiv -1 \pmod 4 \text{ für ungerades } \bar{a}, \quad 4 | D \text{ für gerades } \bar{a}.$$

$4 | D$ ist unmöglich. Bezeichnet v die Anzahl der ungeraden Primteiler von D, so beträgt also die Anzahl der ambigen Formen für $D \equiv 1 \pmod 4$ mindestens 2^v, für $D \equiv 2, -1 \pmod 4$ mindestens 2^{v+1} (für $D \equiv -1 \bmod 4$ ist zugleich $\varrho = 0, 1$ möglich).

III. Jeder binären quadratischen Form $ax^2 + bxy + cy^2$ der Determinante $4D$ ordnen wir ihre Charaktere $\left(\frac{m}{p}\right)$, $(-1)^{t(m)}$ zu, wo m eine durch $ax^2 + bxy + cy^2$ darstellbare Zahl bezeichnet, $t(m)$ ein gewisses Polynom, $(m, 2D) = 1$ und n ungerader Primteiler von D ist. Sie sind nur von der Form $ax^2 + bxy + cy^2$ abhängig; dabei ist ihre Anzahl für $D \equiv 1 \pmod 4$ gleich v, für andere D gleich $v + 1$ [5]). Die binären quadratischen Formen, denen dasselbe Charakterensystem entspricht, bilden ein Geschlecht. Diejenigen, bei denen die Charaktere sämtlich gleich 1 sind, bilden das Hauptgeschlecht. Offenbar gehört das Quadrat einer beliebigen Form zum Hauptgeschlecht. Nach einem Gaußschen Satze [6]) ist auch umgekehrt jede Form des Hauptgeschlechts Quadrat einer anderen Form. Durchläuft also C_i^2 $(i = 1, 2, \ldots)$ sämtliche verschiedenen Quadrate der Formen der Diskriminante $4D$, so ist jede Form derselben Diskriminante einer Form αC_i gleich, wo α^2 die Einheitsform ist. Bezeichnet also H die Klassenzahl der Determinante $4D$, A die Anzahl der ambigen Formen und h die Anzahl der Formen des Haupt-

---

[4]) Vgl. z. B. E. Cahen, Theorie des Nombres II, Paris 1924, S. 324—326.

[5]) Vgl. z. B. Cahen, a. a. O. [4]) S. 397—399.

[6]) Vgl. z. B. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie (1894), §§ 155—158, oder H. Hasse, Elementarer Beweis des Hauptsatzes über ternäre quadratische Formen mit rationalen Koeffizienten, Journ. f. d. r. u. a. Math. **172** (1935), S. 129—132.

geschlechtes, so ist $H = Ah$. Andererseits ist $H = gh$, wo g die Anzahl der Geschlechter von $4D$ bedeutet. Also ist $A = g$. Nun erhält man aus dem Reziprozitätsgesetz unmittelbar, daß das Produkt sämtlicher Charaktere gleich 1 ist [7]). Demnach ist die Anzahl der Geschlechter für $D \equiv 1 \pmod 4$ höchstens gleich 2^{v-1}, für andere D höchstens gleich 2^v. Wir erhalten also einen Widerspruch zu II.

Satz 5 [8]). *Ist D eine quadratfreie natürliche Zahl, so ist eine und nur eine der Gleichungen*

$$D_1 u^2 - D_2 v^2 = \varepsilon, \quad \varepsilon = \pm 1, \pm 2, \quad D_1 D_2 = D, \quad D_1 < D_2, \tag{2}$$

wo $\varepsilon = -1$ für $D_1 = 1$, in natürlichen Zahlen u, v lösbar.

Beweis. I. Zunächst bemerken wir, daß mindestens eine der Gleichungen (2) lösbar ist. Um dies einzusehen, betrachten wir die kleinsten natürlichen Zahlen t, w, für die $t^2 - Dw^2 = 1$ ist. Man erhält dann, daß für gewisse ganze rationale Zahlen α, β, D_1, D_2, v_1, v_2

$$t + 1 = 2^\alpha D_1 v_1^2, \quad t - 1 = 2^\beta D_2 v_2^2, \quad D = D_1 D_2, \quad 0 \leqq \alpha + \beta \leqq 2.$$

Also ist $2 = 2^\alpha D_1 v_1^2 - 2^\beta D_2 v_2^2$ eine Gleichung vom Typus (2).

II. Es sei $D_1 x^2 - D_2 y^2$ die Form aus I, für die $D_1 x^2 - D_2 y^2 = \varepsilon$ lösbar ist. Demnach erhält man sämtliche Lösungen der Pellschen Gleichung $x^2 - Dy^2 = 1$ aus $\left(\frac{\sqrt{D_1}x + \sqrt{D_2}y}{\sqrt{|\varepsilon|}}\right)^{2k}$, wo k eine ganze rationale Zahl bezeichnet. Wäre $d_1 x^2 - d_2 y^2 = \varepsilon_1$, $\varepsilon_1 = \pm 1, \pm 2$ eine andere Lösung von (2), so würde für eine gewisse ganze rationale Zahl n

$$\frac{\sqrt{d_1}x \pm \sqrt{d_2}y}{\sqrt{|\varepsilon_1|}} = \pm\left(\frac{\sqrt{D_1}x + \sqrt{D_2}y}{\sqrt{|\varepsilon|}}\right)^n$$

sein, denn $\left(\frac{\sqrt{d_1}x + \sqrt{d_2}y}{\sqrt{|\varepsilon_1|}}\right)^2$ ergibt wieder eine Lösung der Pellschen Gleichung. Mithin hat (2) höchstens eine Lösung.

---

[7]) Vgl. z. B. Cahen, a. a. O. [4]), S. 399—403; nach Hilbert ist dies der eigentliche Sinn des Reziprozitätsgesetzes.

[8]) K. Petr, Über die Pellsche Gleichung, Časopis **56** (1927), S. 57—66.

Eingegangen 2. Juni 1936.